

INSYS Locks

**B** BREMER  
TRESOR

TwinLock B7X0 Business LS  
TwinLock C8X0 Business LS  
TwinLock D9X0 Business LS  
Basis- und Komfortsysteme

---



# Impressum

Copyright © September 2023 INSYS MICROELECTRONICS GmbH

Der Inhalt dieser Anleitung ist urheberrechtlich geschützt. Seine Verwendung ist im Rahmen der Nutzung des Systems zulässig. Eine darüber hinaus gehende Verwendung ist ohne schriftliche Genehmigung des Herstellers nicht gestattet. Für Kritik und Anregungen sind wir jederzeit dankbar. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

Bei der Zusammenstellung der Texte wurde mit größter Sorgfalt vorgegangen. Trotz aller Bemühungen kann es zu Abweichungen gegenüber den tatsächlichen Funktionen kommen. Für die Richtigkeit des Inhalts kann daher keine Gewährleistung übernommen werden. Für unkorrekte Angaben und deren Folgen können wir weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise sind wir jederzeit dankbar.

Das Design der TwinCard Karten kann von dem gegebenenfalls abgebildeter Musterkarten abweichen. Gleiches gilt für das Design der grafischen Benutzeroberfläche von Programmen.

## *Warenzeichen und Firmenzeichen*

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

Windows<sup>®</sup> ist ein Warenzeichen von Microsoft Corporation.

INSYS locks<sup>®</sup> ist eine Marke der INSYS MICROELECTRONICS GmbH.

## *Herausgeber*

INSYS MICROELECTRONICS GmbH

Hermann-Köhl-Str. 22

93049 Regensburg, Deutschland

Internet: <http://www.insys-locks.com>

Technische Änderungen, Auslassungen sowie Irrtum vorbehalten.

## Zulassungen



EN1300  
M114307 Hochsicherheitsschloss – Klasse 2 (TwinLock B7X0 Business)  
M114308 Hochsicherheitsschloss – Klasse 3 (TwinLock C8X0 Business)  
M116305 Hochsicherheitsschloss – Klasse 4 (TwinLock D9X0 Business)  
G106016 TwinXT Sperreinrichtung - Klasse C  
G105133 TwinAlarm Schalteinrichtung - Klasse C  
G108061 TwinXT Überfallmelder – Klasse C  
G108062 TwinAlarm Überfallmelder – Klasse C  
G114106 TwinXT Verschlussüberwachung – Klasse C  
G114107 TwinAlarm Verschlussüberwachung – Klasse C



EN 1300  
Hochsicherheitsschloss Klasse B  
Hochsicherheitsschloss Klasse C  
Hochsicherheitsschloss Klasse D

Achtung!  
Vor der Montagesorgfältig lesen.  
Aufbewahren zum späteren Nachschlagen.



Ihre Meinung ist uns wichtig. Bitte bewerten Sie uns.

DE: <https://www.insys-locks.com/de/kundenzufriedenheit/>

# Inhaltsverzeichnis

1	Zu dieser Dokumentation .....	7
1.1	Inhalte und Nutzung .....	7
1.2	Benutzerqualifikation .....	7
1.3	Textauszeichnungen und Formatierung .....	8
1.3.1	Sicherheitshinweise .....	8
1.3.2	Symbolbedeutungen .....	9
1.3.3	Handlungsanweisungen .....	10
2	Sicherheit .....	11
2.1	Bestimmungsgemäßer Gebrauch .....	11
2.2	Gefahren durch elektrische Energie .....	11
2.3	Verantwortung des Betreibers .....	11
2.4	Personalanforderungen .....	12
2.4.1	Qualifikationen .....	12
2.4.2	Definition „Elektrofachkraft“ .....	12
2.5	Umweltschutz .....	12
3	Systembeschreibung .....	13
3.1	TwinLock B7X0/C8X0/D9X0 Business LS .....	13
3.1.1	Systemaufbau .....	14
3.1.2	Bedieneinheit FlatControl .....	19
3.1.3	Schloss INSYS Lock 700 / -800 / -900 .....	19
3.1.4	Busverteiler TwinConnect / TwinConnect small .....	20
3.1.5	Sperreinrichtung TwinXT / TwinXT small / TwinXT II .....	20
3.1.6	Schalteinrichtung TwinAlarm .....	21
3.1.7	RFID Karten .....	21
3.1.8	Chipkarten TwinCard .....	22
3.1.9	Übersicht: Codes im System .....	23
3.2	Funktionsübersicht .....	24
3.2.1	Allgemeine Funktionen .....	24
3.2.2	Mit optionaler Software einstellbare Funktionen .....	26
3.2.3	Optionale Funktionen ab Version LP09 .....	27
3.2.4	Optionale Funktionen ab Version LP10 .....	28
3.2.5	Optionale Funktionen ab Version LP11 .....	28
3.2.6	Optionale Funktionen ab Version LP/LQ12 .....	31
3.2.7	Optionale Funktionen ab Version LP/LQ14 .....	32
4	Bedienung .....	34
4.1	Bedienelemente Bedieneinheit FlatControl .....	34
4.2	Hotkeys .....	35
4.3	Konfiguration mit PC Software TwinComm .....	35
4.4	Betrieb mit abhängigen Einmalcodes .....	36
4.4.1	Voraussetzungen für abhängigen Einmalcode .....	36
4.5	Systemstatus .....	37
4.6	Benutzer- / Personalnummern .....	38
4.6.1	Benutzer- / Personalnummer eingeben .....	38
4.7	Benutzergruppen .....	39
4.7.1	Bedienung mit „Benutzergruppen“ aktiviert .....	39
4.7.2	Master / WTU-Master wählen .....	40

4.8	Benutzer autorisieren.....	40
4.8.1	Felder und Kontrollkästchen der Benutzermatrix.....	41
4.8.2	Werkseinstellung Rechte Benutzermatrix.....	42
4.8.3	Berechtigungen Manager / Master / Benutzer.....	43
4.9	Menüführung in der Bedieneinheit.....	44
4.9.1	TwinLock BC7X0 Business.....	44
4.10	PIN-Codes.....	45
4.10.1	Arten und Anzahl von PIN-Codes in jedem Schloss.....	46
4.10.2	PIN-Code eingeben.....	47
4.10.2.1	PIN-Code mit Menütasten eingeben.....	47
4.10.2.2	PIN-Code mit Zifferntasten eingeben.....	47
4.11	RFID Karten und Chipkarten.....	48
4.11.1	RFID Karten.....	48
4.11.2	RFID Karte mit Bedieneinheit / Leser einlesen.....	49
4.11.3	Codekarte TwinCard code access.....	50
4.11.4	Chipkarten TwinCard configuration II / - language.....	50
4.11.5	Chipkarte in FlatControl / in Leser einlegen.....	50
4.12	Öffnen und Schließen.....	51
4.12.1	Schloss mit PIN-Code öffnen.....	51
4.12.2	Zusätzlich mit Codekarte öffnen.....	52
4.12.3	Beim Öffnen Stillen Alarm auslösen.....	53
4.12.4	Schloss mit Codeverknüpfung öffnen.....	54
4.12.5	Schloss mit Öffnungsverzögerung öffnen.....	54
4.12.6	Mit Öffnungsverzögerung und Freigabezeit öffnen.....	55
4.12.7	Schlösser mit Parallelcode öffnen.....	55
4.12.8	Schloss mit abhängigem Einmalcode öffnen.....	56
4.12.9	Einbruchmeldeanlage (EMA) unscharf schalten.....	56
4.12.10	Schloss schließen.....	57
4.12.11	Schloss mit Code-Eingabe schließen.....	57
4.12.12	Mit Türschalter automatisch schließen.....	58
4.12.13	Automatisches Schließen TK.....	58
4.12.14	Einbruchmeldeanlage (EMA) scharf schalten.....	59
4.13	System einrichten.....	60
4.13.1	Verstecktes Menü anzeigen.....	60
4.13.2	Einstellungen: Schlosssystem.....	61
4.13.2.1	Codeverknüpfung.....	61
4.13.2.2	Parallelcode.....	61
4.13.2.3	Zwangsfolge.....	62
4.13.2.4	Zeitverzögerung.....	62
4.13.2.5	Wochenprogramme.....	62
4.13.3	Datum und Uhrzeit einstellen.....	63
4.13.4	Alarmgeräte einstellen / ein- / ausschalten.....	64
4.13.5	WTU-Funktion / Zwei ‚Benutzergruppen‘ wählen / Zähler-Reset.....	65
4.14	Verwaltung und Benutzer.....	66
4.14.1	Systemmanagercode ändern.....	66
4.14.2	Mastercode / WTU-Mastercode ändern.....	67
4.14.3	PIN-Code für Benutzer anmelden.....	68
4.14.4	PIN-Code ändern.....	70
4.14.5	PIN-Code abmelden.....	71
4.14.6	PIN-Code Benutzer-Anzeige.....	72
4.14.7	Codekarte anmelden (auch RFID-Karten).....	73
4.14.8	Codekarte abmelden (auch RFID-Karten).....	74
4.14.9	Codekarte Benutzer-Anzeige (auch RFID Karten).....	75

4.15	Service .....	76
4.15.1	Status / Info des Systems anzeigen .....	76
4.15.2	Service Reset .....	77
4.15.3	Motor-Service / Motor Schritt.....	79
4.15.4	Schloss anmelden .....	80
4.15.4.1	Zusätzliches Schloss .....	80
4.15.4.2	Schloss wechseln .....	81
4.15.5	System bei defektem Riegelwerkskontakt verschließen.....	82
4.15.6	Lizenzierung .....	82
4.15.7	Schnell- / Eilsperre in Kraft setzen .....	83
4.16	Import / Export.....	84
4.16.1	Protokoll exportieren .....	84
4.16.2	Protokoll anzeigen / drucken .....	85
4.16.3	Konfiguration importieren .....	86
4.16.4	Meldungen beim Import der Konfiguration .....	87
4.16.5	Konfiguration exportieren.....	89
4.16.6	Sprache wählen.....	89
4.16.7	Sprache importieren.....	90
5	Wartung, Reparatur und Reinigung .....	91
6	Störungsabhilfe .....	92
6.1	System bei Netzausfall mit Spannung versorgen .....	92
6.2	Fehlermeldungen.....	92
7	Technische Unterstützung .....	98
8	Entsorgung .....	98
9	Glossar .....	99
10	Anhang.....	106
10.1	Abbildungsverzeichnis.....	106
10.2	Notizen .....	107

# 1 Zu dieser Dokumentation

## 1.1 Inhalte und Nutzung

Dieses Handbuch enthält Informationen zu Betrieb, Konfiguration und Pflege des Hochsicherheitsschlosssystems TwinLock B7X0 / C8X0 / D9X0 Business LS (lokales System).

Es beschreibt die Bedienvorgänge für die Systemvarianten der VdS-Klassen 2, 3 und 4 und bietet Informationen zu den Einstellungen. VdS Schadenverhütung GmbH ist ein Unternehmen der deutschen Versicherungswirtschaft, das unter anderem Produkte aus dem Bereich der Sicherheitstechnik evaluiert.

Zur Menüführung siehe Abschnitt „Menüführung in der Bedieneinheit“ auf Seite 44, zu den Berechtigungen siehe „Berechtigungen Manager / Master / Benutzer“ auf Seite 43.

Für Systeme TwinLock B7X5 Business gibt es ein eigenes Handbuch.

Informationen zu Montage und Inbetriebnahme finden Sie in der Montageanleitung des Systems.

Anleitungen zu Öffnungs- und Schließvorgängen enthält die Kurzbedienungsanleitung.

Diese Anleitungen ermöglichen den sicheren und effizienten Umgang mit dem System. Sie sind Bestandteil des Systems. Die jeweils benötigte Anleitung muss in aktueller Version für Fachkräfte / Personal jederzeit zugänglich nahe beim System aufbewahrt werden.






Der Betreiber eines jeden Systems, das im gewerblichen Bereich eingesetzt wird, hat dafür zu sorgen, dass die Unfallverhütungs- und Umweltschutz-Vorschriften sowie die allgemeinen Sicherheitsbestimmungen für den Einsatzbereich des Systems eingehalten werden.

## 1.2 Benutzerqualifikation

Dieses Handbuch richtet sich vor allem an qualifizierte und geschulte Fachkräfte. Einrichter und Verwalter von TwinLock müssen fähig und auch sprachlich in der Lage sein, dieses Handbuch zu lesen und zu verstehen, um sich mit den Einrichtungs-, Verwaltungs- und Bedienvorgängen vertraut machen und das System richtig konfigurieren, bedienen sowie Störungen beheben und so den sicheren Betrieb des Systems gewährleisten zu können.

## 1.3 Textauszeichnungen und Formatierung

### 1.3.1 Sicherheitshinweise

	<p><b>Gefahr</b></p> <p>Unmittelbare Lebensgefahr / Gefahr der schweren Körperverletzung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.</p>
	<p><b>Warnung</b></p> <p>Mittelbare Lebensgefahr / Gefahr der schweren Körperverletzung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.</p>
	<p><b>Vorsicht</b></p> <p>Verletzungsgefahr. Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.</p>
	<p><b>Vorsicht</b></p> <p>Gefahr eines Sachschadens Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.</p>
	<p><b>Hinweis</b></p> <p>Keine Gefahrenmeldung, sondern Zusatzinformation. Hintergrundinformation / Tipps.</p>

### 1.3.2 Symbolbedeutungen



Benützen Sie die Bedieneinheit.



Für die folgenden Schritte benötigen Sie Werkzeug.



Für die folgenden Schritte benötigen Sie einen PIN-Code für Benutzer.



Für die folgenden Schritte benötigen Sie einen Mastercode.



Für die folgenden Schritte benötigen Sie den Systemmanagercode (Managercode des Schlosses 1).



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte Card code access.



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte Card configuration II.



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte Card language.



Für die folgenden Schritte benötigen Sie eine optionale RFID Karte.



Symbole für ungesicherten / gesicherten Bereich in Abbildungen.

### 1.3.3 Handlungsanweisungen

Text ohne besondere Formatierung gleich nach der Überschrift einer Handlungsanweisung enthält nicht sicherheitsrelevante Hinweise auf Umstände, die bei der Ausführung der Handlung zu beachten sind.

**Sie benötigen** Text, dem 'Sie benötigen' vorangestellt ist, enthält Hinweise zu Werkzeugen oder anderen Mitteln, die Sie für die erfolgreiche Durchführung der Handlungsschritte benötigen. Achten Sie auch auf die abgebildeten Symbole.

**Vorbedingung** Text, dem 'Vorbedingung(en)' vorangestellt ist, enthält Bedingungen, die erfüllt sein müssen, bevor Sie die Handlungsschritte ausführen können.

1. So formatierter Text fordert Sie auf, etwas zu tun. Er kann die Namen von Tasten und auf der Bedieneinheit angezeigten Displaytext enthalten.

*So formatierter Text enthält Resultate, die die Folge davon sind, dass Sie einen Handlungsschritt ausgeführt haben.*

So formatierter Text am Ende einer Handlungsanweisung zeigt Ihnen, dass Sie das Ziel Ihrer Handlung erreicht haben.

## 2 Sicherheit

Dieser Abschnitt bietet einen Überblick der Gesichtspunkte, die zum Schutz von Personen und für einen sicheren und störungsfreien Betrieb des Systems zu beachten sind. Weitere aufgabenspezifische Sicherheitshinweise finden Sie in den nachfolgenden Kapiteln vor der Beschreibung der Handlungsschritte, für die die jeweiligen Hinweise zu beachten sind.

### 2.1 Bestimmungsgemäßer Gebrauch

#### Warnung



Gefahr des Einschließens von Personen.  
 Lebensgefahr durch Nahrungs- / Luftmangel.  
 Stellen Sie vor dem Schließen jedes Schlosses sicher, dass sich keine Personen in dem zu verschließenden Behältnis / Raum befinden.

Verwenden Sie das Hochsicherheitsschlosssystem TwinLock Business ausschließlich zum Öffnen und Schließen Ihres Wertbehältnisses sowie zur Verwaltung der Öffnungs- und Schließvorgänge.

### 2.2 Gefahren durch elektrische Energie

In der Montageanleitung beschriebene Arbeiten, für die Gehäuse von Einheiten des Systems geöffnet werden müssen, dürfen ausschließlich von Elektrofachkräften (Definition siehe S. 12), die von INSYS MICROELECTRONICS oder berechtigten Partnerunternehmen geschult und autorisiert wurden, durchgeführt werden.

#### Vorsicht

Gefahr von Kurzschluss der elektronischen Komponenten.  
 Gefahr der Beschädigung des Systems  
 Beachten Sie die Anweisungen zur Reinigung des Systems.  
 Führen Sie Arbeiten an Hardwarekomponenten durch wie in der Montageanleitung beschrieben. Eigenmächtige Umbauten und Änderungen sind verboten.

### 2.3 Verantwortung des Betreibers

Wenn das Hochsicherheitsschlosssystem im gewerblichen Bereich eingesetzt wird, unterliegt der Betreiber des Systems den gesetzlichen Pflichten zur Arbeitssicherheit.

Neben den Sicherheitshinweisen in dieser Anweisung müssen die für den Einsatz des Systems am Einsatzort gültigen Sicherheits-, Unfallverhütungs- und Umweltschutzvorschriften eingehalten werden.

## 2.4 Personalanforderungen

### 2.4.1 Qualifikationen

Die verschiedenen in dieser Anleitung beschriebenen Aufgaben stellen unterschiedliche Anforderungen an die Qualifikation der Personen, die mit diesen Aufgaben betraut sind.

#### Warnung



Gefahr bei unzureichender Qualifikation von Personen, die das System einrichten.

Unzureichend qualifizierte Personen können die Risiken beim Umgang mit unter Spannung stehenden Elementen nicht richtig einschätzen.

Alle Arbeiten, für die Gehäuse oder Isolierungen von Bestandteilen des Systems entfernt werden müssen, nur von geschulten Elektrofachkräften ausführen lassen.

Unzureichend qualifizierte Personen während solchen Arbeiten aus dem Arbeitsbereich fernhalten.

Ausschließlich von INSYS MICROELECTRONICS oder einem Partnerunternehmen autorisierte und am System geschulte Elektrofachkräfte dürfen Arbeiten ausführen, bei denen die Hardware-Komponenten des Systems geöffnet werden müssen oder die Hardware-Konfiguration verändert wird.

### 2.4.2 Definition „Elektrofachkraft“

Eine Elektrofachkraft ist aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie der Kenntnis der einschlägigen Normen und Bestimmungen in der Lage, Arbeiten an elektrischen Anlagen auszuführen und mögliche Gefahren selbstständig zu erkennen und zu vermeiden.

Sie ist speziell für das Arbeitsumfeld, in dem sie tätig ist, ausgebildet und kennt die relevanten Normen und Bestimmungen.

## 2.5 Umweltschutz

Der Betreiber hat dafür Sorge zu tragen, dass alle am Einsatzort gesetzlich relevanten, den Umweltschutz betreffenden Aspekte während des gesamten Lebenszyklus des Produktes beachtet werden.

Siehe auch Kapitel „Entsorgung“ auf Seite 98.

## 3 Systembeschreibung

### 3.1 TwinLockB7X0/C8X0/D9X0 Business LS

Die allgemeine Produktbezeichnung ist TwinLockB7XX / C8XX / D9X0Business X.X LS.

„TwinLock“ bezeichnet dabei die Produktreihe, „Business LS“ den Produkttyp. Der der Zahlenfolge vorangestellte Buchstabe steht für die VdS Klasse. B steht für Klasse 2, C für Klasse 3 und D für Klasse 4.

Die erste Zahl, „7“, beziehungsweise „8“ oder „9“ steht für das Schlossmodell.

Das erste „X“ steht für „0“, „1“, „2“, „3“ oder „4“, für die Version ohne / mit RFID:

0 = ohne RFID

1 = mit RFID, Hitag (LF), 125 KHz

2 = mit RFID, Mifare classic (HF), 13,56 MHz

3 = mit RFID, Legic (HF), 13,56 MHz

4 = mit RFID, Mifare Classic / DESFire, 13,56 MHz

Das zweite „X“ kann die Werte „0“ oder „5“ annehmen. „0“ kennzeichnet Systeme mit Standardfunktionen, bei denen mit geeigneter Firmware auch abhängiger Ein-

malcode (OTC) verwendet werden kann. „5“ steht für Systeme, bei denen optional flexibler Einmalcode verwendet werden kann. Für diese Systeme (B7X5) gibt es ein separates Handbuch.

Die erste Ziffer [X] hinter „Business“ gibt die Zahl der Schlösser im System an, die zweite Ziffer zeigt an, wie viele Sperreinrichtungen TwinXT (II) / TwinXT small (keine, „1“ oder „2“) Teil des Systems sind.

TwinLock B7X0 / C8X0 C9X0 Business ist ein modular aufgebautes elektronisches Hochsicherheitsschlosssystem, bei dem die sicherheitsrelevanten Komponenten voll redundant ausgeführt sind.

Es ist ein Schlosssystem mit mindestens bis zu 100 direkt am Schloss gespeicherten Benutzern. Mit Softwareversion xx0 können diese Benutzer eine Gruppe bilden oder in zwei Gruppen für zwei Mandanten (beispielsweise Geldinstitut und Werttransport- unternehmen) aufgeteilt werden. Die Benutzer können sich durch PIN-Code und gegebenenfalls zusätzlich durch Karten (mit Chip oder RFID) authentifizieren.

Ein System enthält eine Bedieneinheit FlatControl, mindestens ein Schloss INSYS Lock 700 / 800 / 900 und einen Busverteiler TwinConnect / TwinConnect small, der die Komponenten verbindet. Alle Systeme enthalten außerdem ein Handbuch.

Komfortsysteme enthalten 1 Schalteinrichtung TwinAlarm.

Basissysteme enthalten bis zu 2 Sperreinrichtungen TwinXT (II) / TwinXT small.

Mit TwinLock D9X0 der VdS-Klasse 4 sind maximal 10 Eingabefehler pro Stunde erlaubt.

## 3.1.1 Systemaufbau

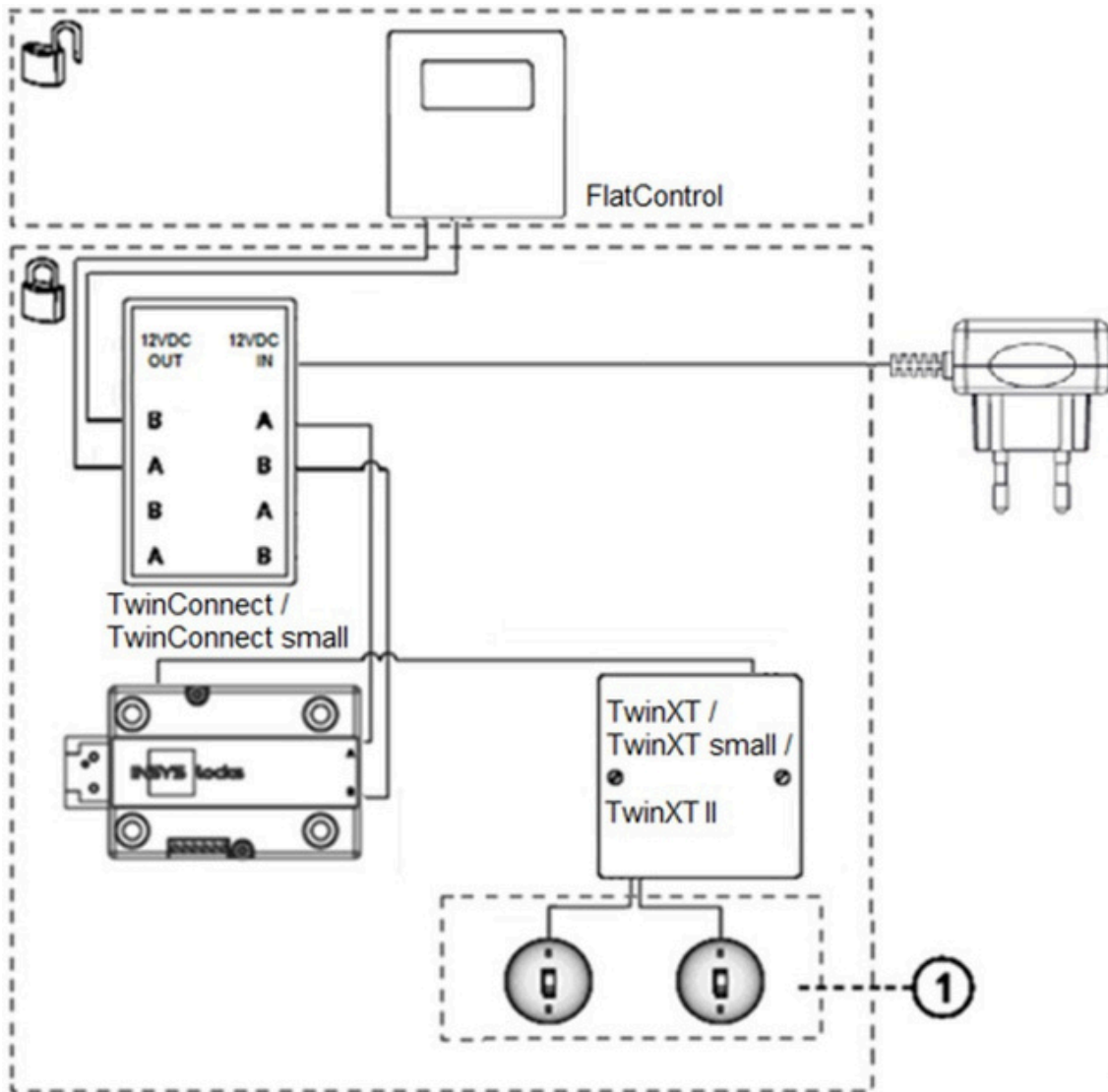


Abb. 1: Systemaufbau von Basissystem 1.1

1) Zwei optionale Schalter für Riegelwerk und Schloss-Freigabe

Das Basissystem 1.1 besteht aus einer Bedieneinheit, einem Netzteil im ungesicherten Bereich, einem Schloss INSYS Lock 700 / 800 beziehungsweise INSYS Lock 900, einem Busverteiler TwinConnect sowie der Sperreinrichtung TwinXT oder TwinXT II im gesicherten Bereich. TwinConnect und TwinXT können auch als Variante „small“ ausgeführt sein.

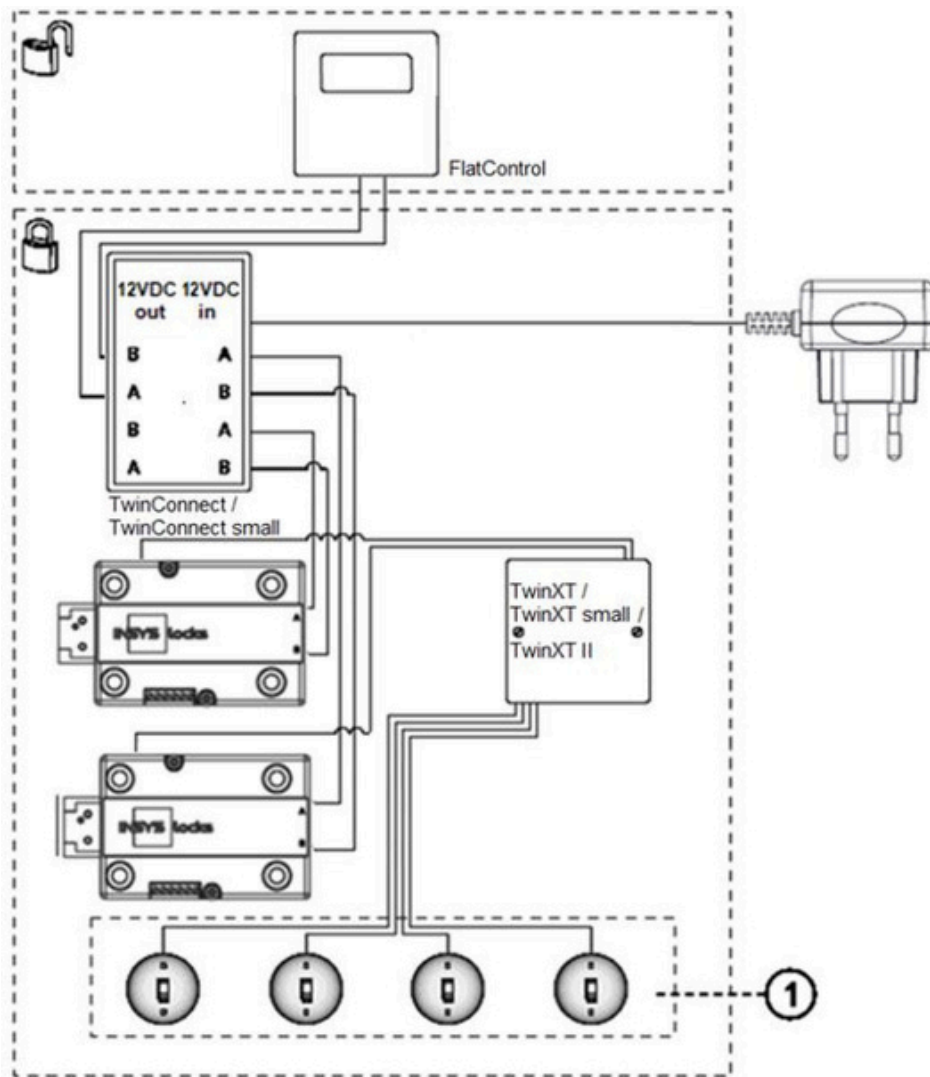


Abb. 2: Systemaufbau von Basissystem 2.1

- 1) Je zwei optionale Schalter für Riegelwerk und Schloss-Freigabe

Das Basissystem 2.1 enthält im gesicherten Bereich zwei Schlösser. Alle anderen Komponenten entsprechen denen von Basissystem 1.1.

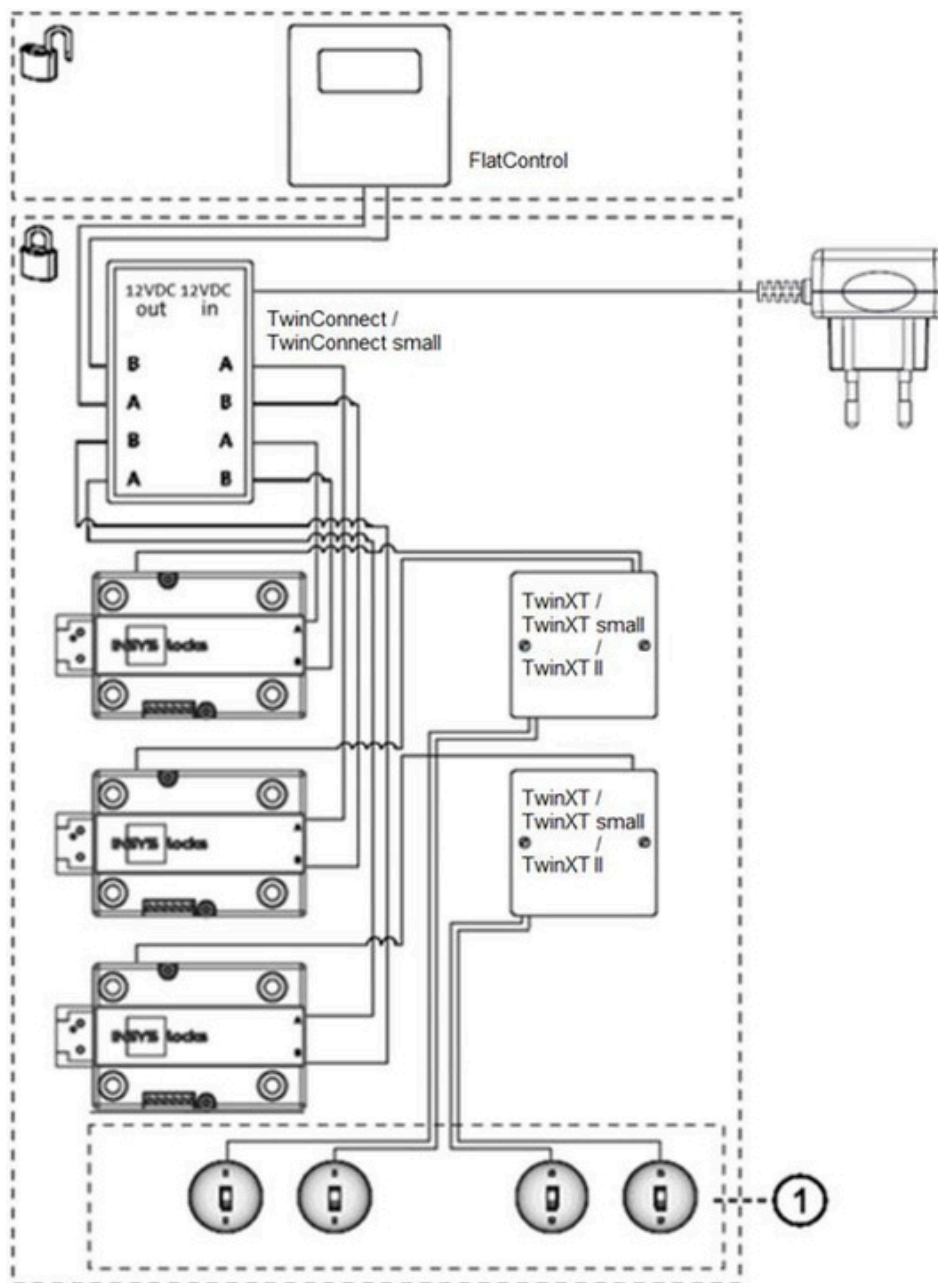


Abb. 3: Systemaufbau von Basissystem 3.2

- 1) Je zwei optionale Schalter für Riegelwerk und Schloss-Freigabe

Das Basissystem 3.2 enthält im gesicherten Bereich drei Schlösser und zwei Sperreinrichtungen TwinXT / TwinXT small oder TwinXT II. Alle anderen Komponenten entsprechen denen von Basissystem 1.1.

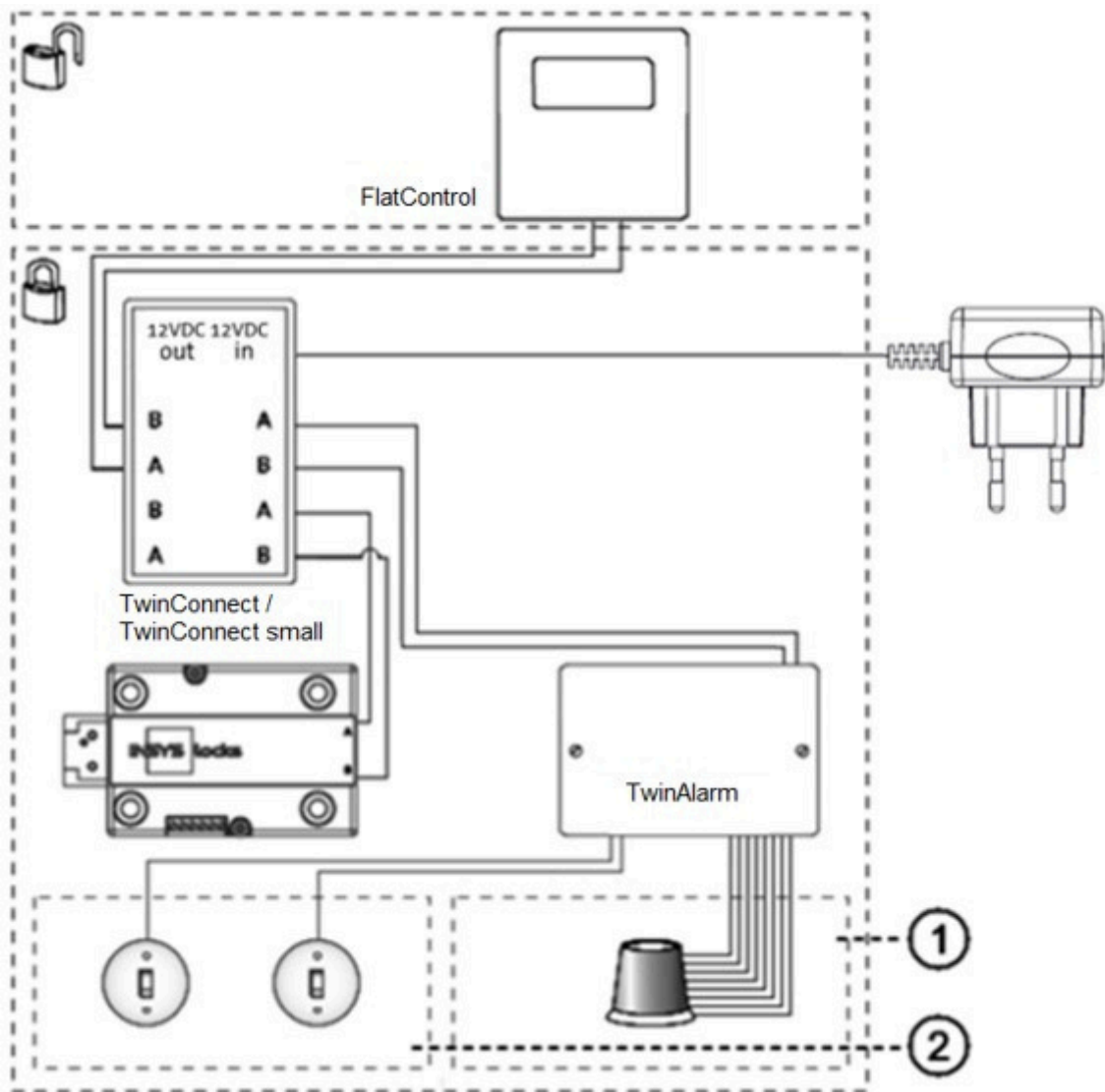


Abb. 4: Systemaufbau von Komfortsystem 1 mit EMA

1) Einbruchmeldeanlage (EMA) mit Eingängen (Alarmkontakt, Zustandskontakt, Scharfschaltung) aus Richtung der Schalteinrichtung TwinAlarm und Ausgängen (EMA-Bereit, Unscharf-Sperre, Quittierung, Freigabe-Sperre, Spannungsversorgung) zur Schalteinrichtung TwinAlarm

2) Optionaler Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre für Schloss INSYS Lock 700 / 800 / 900

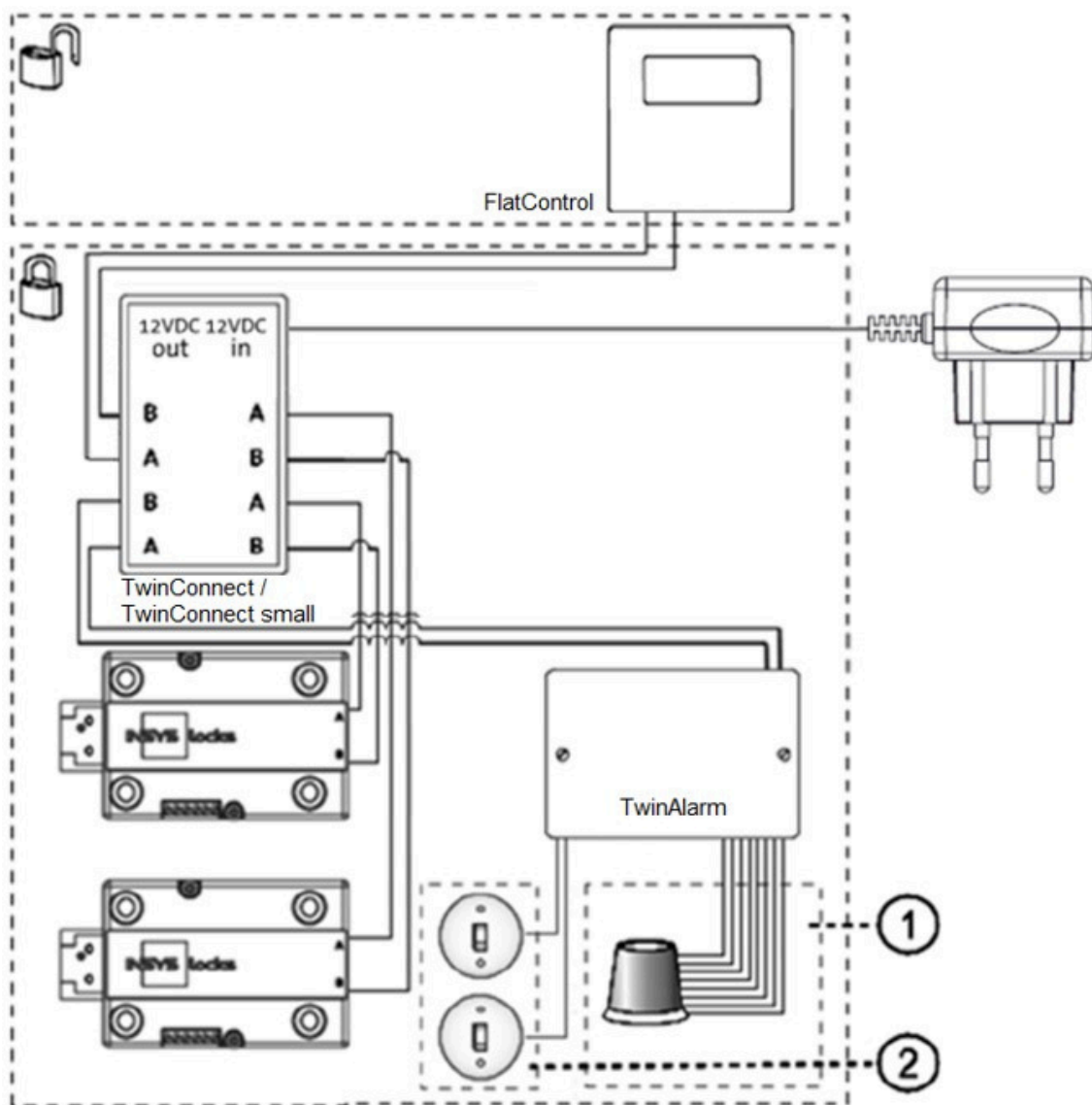


Abb. 5: Systemaufbau von Komfortsystem 2 mit EMA

- 1) Einbruchmeldeanlage (EMA) mit Eingängen (Alarmkontakt, Zustandskontakt, Scharfschaltung) aus Richtung der Schalteinrichtung TwinAlarm und Ausgängen (EMA-Bereit, Unscharf-Sperre, Quittierung, Freigabe-Sperre, Spannungsversorgung) zur Schalteinrichtung TwinAlarm
- 2) Optionaler Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre

### 3.1.2 Bedieneinheit FlatControl



Abb. 6: Bedieneinheit FlatControl

Mit FlatControl können Sie das System TwinLock einstellen und bedienen. Die Bedieneinheit befindet sich im ungesicherten Bereich des Systems. Für eine Beschreibung der einzelnen Bedienelemente siehe Kapitel 4, Bedienung.

Es gibt die Varianten:

FlatControl Business x05, (Standard, ohne RFID)

FlatControl ... x10 für RFID, (125 KHz) / Hitag (LF)

FlatControl ... x20 für RFID, (13,56 MHz) / Mifare Classic (HF)

FlatControl ... x30 für RFID, / Legic (HF)

FlatControl ... x40 für RFID, (13,56 MHz) / DESFire (HF)

### 3.1.3 Schloss INSYS Lock 700 / -800 / -900



Abb. 7: Schloss INSYS Lock 700 VdS2/-800VdS3 / - 900 VdS4

Mit Schloss INSYS Lock 700 (VdS Klasse 2)/-800(VdS Kl. 3)/ - 900 (VdS Kl. 4), können Sie das Wertbehältnis ver- und entriegeln. Das Schloss befindet sich im gesicherten Bereich des Systems. Sie können bis zu 3 Schlösser an das System anschließen.

### 3.1.4 Busverteiler TwinConnect / TwinConnect small

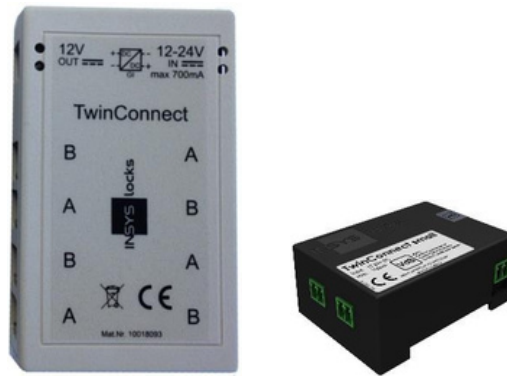


Abb. 8: Busverteiler TwinConnect / TwinConnect small

Über ein redundantes Bussystem verbindet der Busverteiler TwinConnect / Twin-Connect small jeweils 1 Eingabeeinheit und bis zu 3 Schösser. Spannungsversorgung via TwinConnect (small) und Netzteil, gegebenenfalls auch für 1-2 Erweiterungseinheiten TwinXT (II) / TwinXT small oder 1 Schalteinrichtung TwinAlarm. Der Busverteiler befindet sich im gesicherten Bereich des Systems.

### 3.1.5 Sperreinrichtung TwinXT / TwinXT small / TwinXT II



Abb. 9: Sperreinrichtung TwinXT/TwinXT small / TwinXTII

Die optionale Sperreinrichtung TwinXT/TwinXTsmall / TwinXT II im gesicherten Bereich des Systems gibt es nur als Erweiterungseinheit für Basissysteme. Mit einer Einheit small können Sie das SystemumEin-undAusgänge erweitern. Dadurch können bis zu zwei Schösser einzeln gesperrt/freigegeben und mit dem Riegelwerkskontakt versehen werden. Zusätzlich verfügt TwinXT (II) / TwinXT small über einen Zustands- und einen Alarmkontakt für den Stillen Alarm.

### 3.1.6 Schalteinrichtung TwinAlarm



Abb. 10: Schalteinrichtung TwinAlarm

Die optionale Schalteinrichtung TwinAlarm innerhalb des Wertbehältnisses verbindet das System mit einer externen Einbruchmeldeanlage (EMA). Sie dient als Verteiler für die Einbruchmeldeanlage (Riegel-, Tür- und andere Kontakte sowie Widerstandsüberwachung). In TwinAlarm werden die elektronischen Schlüssel (Chipkarten) sowie die Eingangssignale der Einbruchmeldeanlage ausgewertet.

### 3.1.7 RFID Karten



Abb. 11: Design-Beispiel RFID Karte

Optionales Zubehör. Die Codekarte RFID ist der gesicherte, mobile Datenträger für die Benutzer eines Systems mit RFID-Funktionalität. Benutzer können ein Schloss mit PIN-Code oder mit PIN-Code und Karte öffnen. Sie können sich auch mit Karte am System identifizieren.

Damit Benutzer Karten verwenden können, müssen die Benutzer in der Benutzermatrix dazu autorisiert worden sein und der Schlossmaster muss geeignete Karten für die Benutzer anmelden.

### 3.1.8 Chipkarten TwinCard

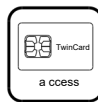


Abb. 12: Symbol "TwinCard code access"

Optionales Zubehör. Die Codekarte TwinCard code access ist ein gesicherter, mobiler Datenträger für die Benutzer des TwinLock Systems. Die Karte kann zusammen mit PIN-Code zur Öffnung genutzt werden.

Damit sich Benutzer die Karte verwenden können, müssen sie in der Benutzermatrix autorisiert worden sein und die Chipkarte muss am Schloss angemeldet worden sein.



Abb. 13: Symbol "TwinCard language"

Optionales Zubehör. TwinCard language ist eine Chipkarte für die Konfiguration der Systemsprache (DE, EN etc.). Sprache und Version sind auf der Karte angegeben. Bei Verwendung einer Karte mit falscher Sprachversion wird eine Fehlermeldung angezeigt.

Verwenden Sie Karten mit Sprachversion v2.xx.

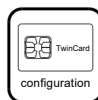


Abb. 14: Symbol "TwinCard configuration II"

Optionales Zubehör. TwinCard configuration II ist eine Chipkarte für die Systemkonfiguration und das Ereignisprotokoll. Das Protokoll kann ausgelesen und ausgewertet werden. Mit der optionalen Software TwinComm können Sie das Schlosssystem via Chipkarte komfortabel konfigurieren und die Konfigurationsdaten speichern.

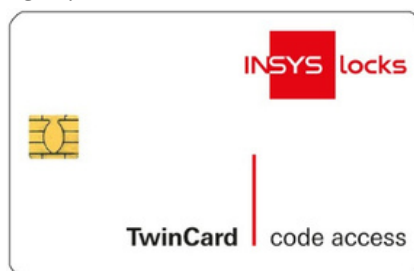


Abb. 15: Design-Beispiel einer Chipkarte TwinCard

## 3.1.9 Übersicht: Codes im System

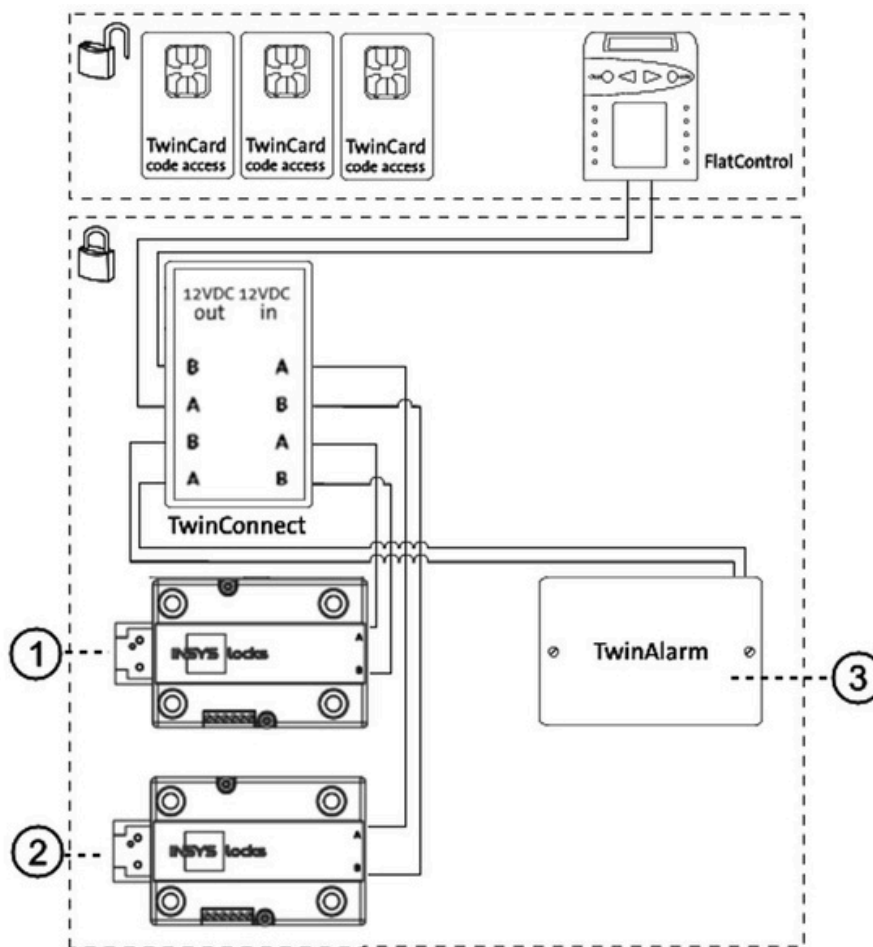


Abb. 16: Übersicht am Beispiel eines Systems mit FlatControl

- 1) Schloss 1: Geistige Codes:  
 1 Systemmanagercode (Managercode von Schloss 1)  
 1 Mastercode  
 99 PIN-Codes für Benutzer
- 2) Schloss 2: Geistige Codes:  
 1 Mastercode  
 99 PIN-Codes für Benutzer
- 3) TwinAlarm: Körperliche Codes:  
 1 Mastercode  
 PIN-Codes für Benutzer

Zusätzlich gibt es gegebenenfalls auf Chipkarten gespeicherte körperliche Codes sowie abhängige und/oder flexible Einmalcodes.

### Vorsicht

Wenn bei Systemen mit TwinAlarm die Benutzercodes vor der Installation / der Aktivierung von TwinAlarm angemeldet werden, werden die Benutzercodes nicht in TwinAlarm gespeichert.

Stellen Sie sicher, dass TwinAlarm installiert und aktiviert ist, bevor Codes / Karten an Schloss 1 angemeldet werden.

## 3.2 Funktionsübersicht

### 3.2.1 Allgemeine Funktionen

Abhängig von Ausführung und Version des Systems TwinLock B7X0 / C8X0 / D9X0 Business LS sind alle oder ein Teil der hier auszugsweise aufgeführten Funktionen vor / nach der Inbetriebnahme fest einstellbar oder mit der Bedieneinheit nachträglich änderbar.

Öffnen und Schließen

Menügeführte Öffnungs- und Schließvorgänge

Menügeführte Verwaltung und Einrichtung

Öffnen mit Codeeingabe oder mit Codeeingabe und Karte

Öffnen / Schließen mit Parallelcode (2-Schloss-Betrieb) /

gemäß 4-Augen-Prinzip

Automatisches Schließen mit Türschalter

Schließen mit Codeeingabe / ohne Authentifizierung

Schnellöffnung

Feste Öffnungs- / Schließreihenfolge wählbar

Codeverwaltung

1 voreingestellter, programmierbarer Systemmanagercode

1 voreingestellter, programmierbarer Mastercode je Schloss

99 programmierbare PIN-Codes für Benutzer je Schloss

Anzeige Benutzerstatus

Parallelcode

Schnellöffnungsberechtigung mit Code

Programmierbare Zwangsfolge

Codeverknüpfung (4-Augencode)

Schutz vor Codemanipulation

Abhängige Einmalcodes (OTC)

Zeitfunktionen

Alarm- / Sabotageverzögerungen

Stiller Alarm

Datums- und Uhrzeitanzeige

Automatische Sommer- / Winterzeitumstellung

Freigabezeit

Öffnungszeitverzögerung

Sondertage

Teilsperzeiten

Wochenprogramme mit Zeitverzögerungen

Komfortfunktionen

Aktivierbare Displaybeleuchtung

Ständige Selbstdiagnose

Spannungsüberwachung

Spracheinstellung flexibel und individuell (mit optionalem Zubehör)

## Servicefunktionen

Ereignisprotokoll 3000 Ereignisse

Im- / Export der Konfiguration per Chipkarte

Systemstatusanzeige

Reset der Systemkomponenten

Versionsabfrage der Systemkomponenten

Systemkomponenten an- / abmelden

Motortest im Schrittbetrieb

Systemzeile frei programmierbar

Not-Spannungsversorgung bei Spannungsausfall

TwinAlarm-Funktionen und EMA-Anbindung (optional)

Schalteinrichtung TwinAlarm (de-)aktivierbar

Anschluss an Einbruchmeldeanlage (EMA)

(Un-)Scharfschaltung der EMA

Stiller Alarm

1 Zustandskontakt (Relais)

1 Freigabekontakt (potentialfrei)

1 Riegelwerkskontakt (potentialfrei)

Anschlussmöglichkeit für je 2 weitere Riegelwerks- und Türkontakte

Erweiterbare Sabotagelinie

Flächenschutz

Türkontakte

Stützpunkte für Widerstandsüberwachung

Funktionen mit Software Version xx0

abhängiger Einmalcode, OTC (mit Firmware LP/LQ14)

### 3.2.2 Mit optionaler Software einstellbare Funktionen

TwinComm ist ein nicht im Lieferumfang enthaltene Parametrierungsset für das System TwinLock Business.

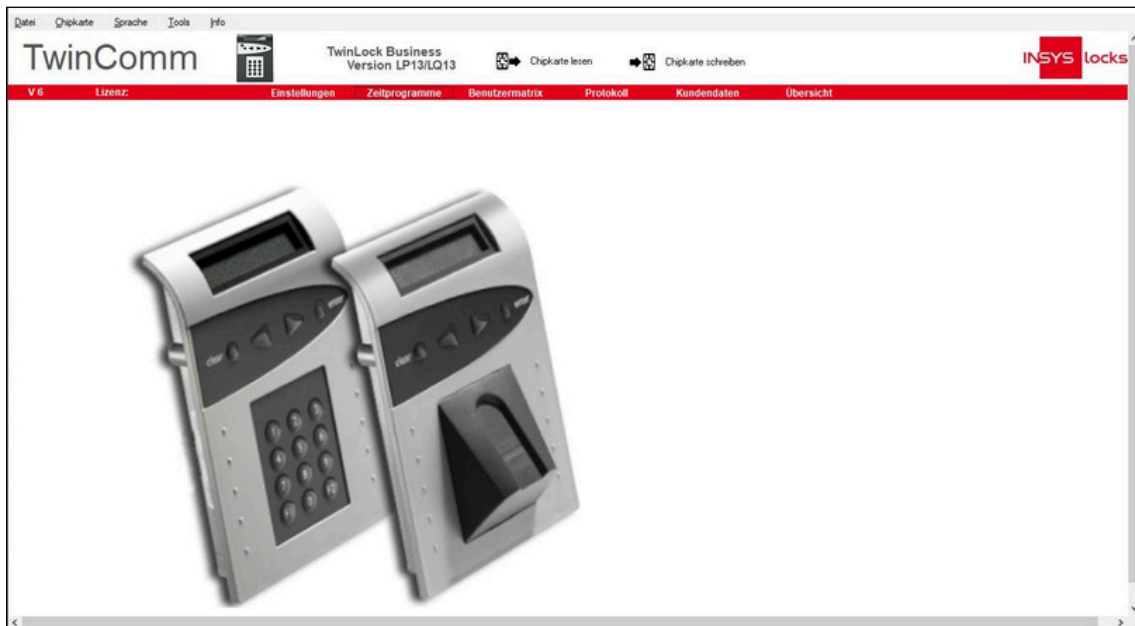


Abb. 17: Beispiel Startseite PC-Software TwinComm

Folgende Funktionen können mit TwinComm programmiert werden:

- Allgemeine Einstellungen
- Automatische Umstellung Sommer- / Winterzeit (de-)aktivierbar
- Einstellung der Batteriewarngrenze (optional)
- Auswertung des Ereignisprotokolls
- Freie Programmierung der 16-stelligen Systemzeile
- Öffnen und Schließen
- Codeverknüpfung gemäß 4-Augen-Prinzip ein- / ausschalten
- Parallelcode (de-)aktivierbar
- Berechtigung für ausgewählte Benutzer, Schloss trotz Zeitprogramm zu öffnen
- Zwangsfolge ein- / ausschalten
- Manuelles Schließen mit Codeabfrage ein- / ausschalten
- Automatisches Schließen mit Türschalter ein- / ausschalten
- Stiller Alarm, auch mit Öffnungsverzögerung ein- / ausschalten
- Codealterung einstellbar
- Optionale Prüfung auf Trivialcode
- Türöffnungsüberwachung
- Öffnungsintervall Schloss 1 – Schloss 2 einstellbar
- Scharf / Unscharf Schalten einer Einbruchmeldeanlage (EMA)
- Zeitprogramme
- Öffnungsverzögerung einstellbar (0-99 Min.)
- Freigabezeit einstellbar (0-99 Min.)
- 5 Wochenprogramme mit Verzögerungen für jeden Wochentag
- Sondertageprogramm für ganztägige Sperrung / Öffnung
- 3 Teilsperrezeiten pro Wochentag
- 10 Sperr- / Öffnungszeiten

Verwaltungsfunktionen  
 Übersicht aller Parameter  
 Protokollanzeige  
 Kundendatenanzeige  
 komfortable Systemkonfiguration  
 Sperreinrichtung TwinXT (II) / TwinXT small (de-)aktivierbar  
 Schalteinrichtung TwinAlarm (de-)aktivierbar  
 EMA-Benutzer (Scharfschaltung) festlegbar  
 Benutzermatrix mit individuellen Autorisierungen einstellbar  
 optionaler zweiter Benutzerbereich mit eigener Verwaltung  
 Öffnungsberechtigung zusätzlich gruppenweise konfigurierbar  
 Anzeige einer Servicetelefonnummer bei Fehlermeldungen  
 Konfiguration der Benutzung von abhängigen Einmalcodes (nur V. XX0, LP14)

### 3.2.3 Optionale Funktionen ab Version LP09

Die Version der Firmware von Bedieneinheit können Sie via Menü **Status / Info** anzeigen. Siehe Seite 76. Einige Funktionen können mit der optionalen PC-Software TwinComm programmiert werden.

Benutzernummern können durch Personalnummern ersetzt werden  
 Lokal (via Benutzermatrix in PC-Software) kann für alle Benutzer eines Systems eingestellt werden, dass sie nicht die systemspezifischen Benutzernummern, sondern ihre 3-6-stelligen Personalnummern eingeben können.

Benutzer können als temporäre Master mit Einmalcode einen neuen Benutzer inklusive PIN-Code und Codekarte anmelden

Lokal via PC-Software (via Registerkarte „Einstellungen“, Bereich „abh. Einmalcodes“, Feld „Master (temp.)“ in TwinComm) kann für Benutzer individuell eingestellt werden, ob sie mit 6-stelligem Einmalcode einen neuen Benutzer anlegen können sollen.

Nach dem Anmelden des neuen Benutzers wird der gültige Bestätigungscode angezeigt, der anschließend gemeldet werden kann. Der jeweils letzte Bestätigungscode kann mit Menü **Status/Info** angezeigt werden.

Betrieb mit zwei Bedieneinheiten

Das Schlosssystem kann mit einer oder mit zwei Bedieneinheiten betrieben werden. Dies wird bei der Installation konfiguriert. Auch für den Betrieb mit zwei Bedieneinheiten ist die VdS-Zulassung gültig.

Achten Sie bei dieser Option besonders auf die Konfiguration der Bedieneinheiten.

Option, den Schlossmaster zu sperren

(Schloss-Öffnung und Anmelden von Benutzern)

Lokal (via Benutzermatrix in PC-Software) kann eingestellt werden, ob der Schlossmaster öffnen (Berechtigung „Öffnen“) beziehungsweise Öffnen / Benutzer anlegen (Berechtigung „Freigabe“) darf.

Stiller Alarm abschaltbar

Lokal (via TwinComm „Einstellungen“, Bereich „Stiller Alarm“, Feld „Stiller Alarm“) kann eingestellt werden, ob Stiller Alarm ausgelöst werden können soll. Falls die Funktion ausgeschaltet wird, kann mit Alarmcode nicht geöffnet werden.

Daten-Export und -Import für ausgewählte Benutzer

bei geöffnetem und bei geschlossenem System

Das entsprechende Menü im Display der Bedieneinheit ist verfügbar und kann verwendet werden unabhängig davon, ob das System geöffnet oder geschlossen ist. Jeder Benutzer mit gültigem PIN-Code kann bei entsprechenden sonstigen Einstellungen Konfigurationsdaten exportieren.

Jeder Benutzer mit Berechtigung „Service“ (via PC-Software) kann Konfigurationsdaten importieren.

Öffnen nach Verzögerung während Freigabezeit nur zu zweit

Lokal kann via Registerkarte „Einstellungen“, Bereich „Codeverknüpfung“, Feld „4-Augen (Freigabe)“ in TwinComm eingestellt werden, ob Benutzer das Schloss in der Freigabezeit nur zu zweit öffnen können sollen.

Ist diese Option gewählt, leitet nur ein Benutzer den Öffnungsvorgang ein.

Einstellung „Zwei Augen“ setzt Einstellung „Parallelcode“ außer Kraft

Lokal (via Kästchen „2 Augen“ in der Benutzermatrix der PC-Software) kann eingestellt werden, dass ein Benutzer die zwei Schlösser eines Schlosssystems auch öffnen darf, wenn die Einstellung „Parallelcode“ für das System gewählt wurde.

Sperrern von Benutzern nach dem Ablauf der Gültigkeit ihres Codes

möglich

Via Bereich „Codealterung/Benutzersperre nach Code-Änderung“ Feld „Zeitraum bis Sperre“ in TwinComm kann eingestellt werden, ob ein Benutzer nach Ablauf der Gültigkeit seines Codes nach einer einstellbaren Anzahl von Monaten automatisch gesperrt und gelöscht wird.

Zeitverzögerung abbrechen

Ausgenommen hiervon sind Alarmzeitverzögerungen und Sperrzeiten. Benutzer können Zeitverzögerungen durch langes Drücken der CLEAR-Taste abbrechen.

### 3.2.4 Optionale Funktionen ab Version LP10

Die Version der Firmware der Bedieneinheit können Sie via Menü Status / Info anzeigen. Siehe Seite 76. Einige Funktionen können mit der optionalen PC-Software TwinComm programmiert werden.

Schnell- / Eilsperre

Für Benutzer, denen ein Wochenprogramm zugeordnet ist, kann durch Drücken von

F2 sowohl bei offenem als auch bei geschlossenem Schlosszustand eine Schnellsperrung programmiert werden. Einmal programmiert, ist für alle zugeordneten Benutzer

das Öffnen im aktuellen Zeitfenster des Wochenprogramms gesperrt. Erst

wenn

das nächste Wochenprogramm beginnt, kann wieder geöffnet werden.

Wochenprogramm-spezifische Verzögerungen

Jedem Wochenprogramm kann eine eigene Öffnungs- und Alarmverzögerung sowie eine Freigabezeit zugeordnet werden.

Manager und Master in Benutzermatrix und Protokoll

Systemmanager und Schlossmaster haben jeweils eigene Einträge in der Benutzermatrix und im Protokoll der PC-Software.

Sondertage auch als Offentage

Sondertage können als „Offentage“ definiert werden, an denen geöffnet werden darf.

### 3.2.5 Optionale Funktionen ab Version LP11

Die Firmwareversion der Bedieneinheit können Sie via Menü Status / Info anzeigen. Siehe Seite 76. Einige Funktionen können mit der optionalen PC-Software TwinComm programmiert werden.

Abhängige Einmalcodes (OTC)

Der Betrieb mit so genannten „abhängigen“ Einmalcodes ist gegebenenfalls möglich. Siehe Abschnitt „Betrieb mit abhängigen Einmalcodes“ auf S. 36.

Zusätzliche Untermenüs zu „Einstellungen“ in Display Bedieneinheit

Menü mit den Untermenüs „Codeverknüpfung“ (4-Augen-Prinzip), „Parallelcode“, „Zwangsfolge“, „Zeitverzögerung“ und „Wochenprogramm“. die oben genannten

Parameter können auch über die Bedieneinheit eingestellt werden (optional via Menü „Schlosssystem“).

#### Interlocking (gegenseitige Verriegelung)

Funktion für Tresore mit zwei Zugängen (Bank / WTU) oder für Tresorraumtür und Tresortür.

##### Interlocking intern aktiv

Markieren Sie das Kontrollkästchen, um das interne Interlocking zu aktivieren.

Dadurch wird von Bank- und WTU-Tür jeweils die Tür gesperrt, die gerade nicht verwendet wird oder die Tresorraumtür wird gesperrt, wenn die Tresortür geöffnet

wird und vice versa.

##### Interlocking extern aktiv

Markieren Sie das Kontrollkästchen, um das externe Interlocking zu aktivieren.

Dadurch wechselt das Schloss den Status schon bei der Code-Eingabe, so dass ab diesem Zeitpunkt niemand mehr den Zugangsraum betreten kann.

##### Systemsperrung / -freigabe

##### Globale Freigabe

Markieren Sie das Kästchen, um die globale Freigabe zu aktivieren. Dadurch bewirken Sie, dass die globale Freigabe / Systemsperrung für das ganze System gilt. Wählen Sie zusätzlich mindestens ein Wochenprogramm, um die Sperrdauer zu definieren. Die Zeiträume, die in den Wochenplänen festgelegt werden können, sind die Zeiträume, in denen die Öffnung erlaubt ist.

##### WP1 / WP2 / WP3 / WP4 / WP5

Markieren Sie Kontrollkästchen, um die Wochenprogramme 1-5 zu aktivieren.

Dadurch bewirken Sie, dass, wenn „Globale Freigabe“ aktiviert ist, gewählte Wochenprogramme für das ganze System und seine Benutzer gelten (Sperrung / Freigabe,

siehe oben) unabhängig davon, ob Benutzer diesen Wochenprogrammen zugeordnet sind oder nicht.

##### Codekarte

Wahl der Art der Codekarte, die Benutzer zum Öffnen verwenden. Mit Einstellung „RFID“ können RFID-Karten verwendet werden.

Wertebereich: 'Chipkarte', 'RFID'. Werkseinstellung: 'Chipkarte'.

##### RFID-Typ

Falls bei „Codekarte“ (siehe oben) oben „RFID“ eingestellt ist, kann hier der RFID-Typ spezifiziert werden.

Wertebereich: 'MIFARE CLASSIC', 'EM4X02', 'EM4X03', 'EM4X05', 'HITAG1', 'HITAG2', 'HITAG5' und 'LEGIC'. Werkseinstellung: 'MIFARE CLASSIC'.

##### Öffnen mit 2 Karten verhindern

Für den Fall, dass für ein 2-Schloss-System „Codeverknüpfung / 4-Augen-Prinzip“ oder „Parallelcode“ und für die Benutzer „1 aus 3“ eingestellt sind. Wählen Sie diese Option, um auszuschließen, dass alle beteiligten Benutzer mit Codekarte

##### Zeitprogrammabbruch aktiv

Markieren Sie das Kontrollkästchen, um den Abbruch von Zeitprogrammen per zusätzlichem Taster aktivieren zu können, falls jemand eingeschlossen sein sollte. Steuerung über Zustand Tür-/ Riegelwerksschalter („offen“) und Zustand Schloss („geschlossen“).

##### Seriennummernvergleich Konfigurationskarte

##### Seriennummernvergleich aktiv

Derzeit nicht verfügbar (09/2023). Markieren Sie das Kontrollkästchen, um den Vergleich der Seriennummern der Geräte mit denen auf der Konfigurationskarte zu aktivieren. Seriennummerneingabe via Kundendaten, Feld ‚Seriennummer‘.

### Codealterung

#### Codealterung [Monate]

Optional fest eingestellt. Einstellung der Anzahl von Monaten, nach denen Benutzer-codes geändert werden sollen. Mit Einstellung „00“ ist der Code uneingeschränkt gültig. Nach Wahl der Option fordert das Programm zur Codeänderung auf. Ab dieser Änderung läuft die hier eingestellte Zeitspanne ab.

#### Codealterung Master [Monate]

Einstellung der Anzahl von Monaten, nach denen der Mastercode ungültig wird. Sonst wie bei „Codealterung [Monate]“, siehe oben.

#### Codealterung Benutzergruppe 2 [Monate]

Einstellung der Anzahl von Monaten, nach denen bei Einstellung „2 Benutzergruppen“ die Codes der zweiten Gruppe ungültig werden. Sonst wie bei „Codealterung [Monate]“, siehe oben.

#### Codealterung Master Benutzergruppe 2 [Monate]

Einstellung der Anzahl von Monaten, nach denen bei Einstellung „2 Benutzergruppen“ der WTU-Mastercode der zweiten Gruppe ungültig wird. Sonst wie bei „Codealterung [Monate]“, siehe oben.

### Erweiterung Kundendaten

Registerkarte „Kundendaten“ ist um die Felder „Seriennummer“, „Tresortyp“, „Objektnummer“, „Inventarnummer“ erweitert worden, über die zusätzliche Daten verarbeitet werden können, was beispielsweise für weitere Sicherheitsfunktionen genutzt wird.

### 3.2.6 Optionale Funktionen ab Version LP/LQ12

Die Firmwareversion der Bedieneinheit können Sie via Menü Status / Info anzeigen. Siehe Seite 76. Einige Funktionen können mit der optionalen PC-Software TwinComm programmiert werden.

Benutzernummern können statt Personalnummern für die An- und Abmeldung von Karten benutzt werden

Beim An- und Abmelden von Karten erfolgt gegebenenfalls eine Abfrage, ob Personalnummern verwendet werden sollen. Wählen Sie gegebenenfalls „Nein“, wenn gewünscht, and „Benutzernummern“.

4-Augen (Öffnen Schloss 2)

Separate Konfiguration des Öffnens nur im 4-Augen-Prinzip für Schloss 2.

Notspannungsüberprüfung

Option der Wahl der Überprüfung der Batteriespannung und gegebenenfalls der Ausgabe von Warnungen.

Automatisches Schließen TK

Option, dass das Schließen automatisch sofort nach dem Schließen der Tür / des Riegelwerks erfolgt, gesteuert vom Türkontakt der Bedieneinheit.

„Personalnummer nicht erkannt“ wird nach der Eingabe einer falschen Personalnummer angezeigt

„Personalnummer nicht erkannt“ statt wie bisher „ungültige Karte“ wird als Fehlermeldung angezeigt, wenn eine falsche Personalnummer eingegeben wird.

Sprachkarten können auch bei geschlossenem System eingelesen werden

Sprachkarten können auch bei geschlossenem System eingelesen werden, wenn die Option „Konfiguration bei geschlossenem System“ eingestellt wurde.

Menüpunkt für Lizenzierung

Die Lizenzierung bestimmter Software kann erfolgen in Menüpunkt „Service / Lizenzierung“.

Nach korrekter Eingabe der Nummer der Software-Lizenz zeigt der entsprechende Wert an, dass das System für die Software lizenziert ist. Wert „00“ bedeutet „nicht lizenziert“.

Hotkeys

Option, bestimmte Tasten der Tastatur der Bedieneinheit als „Hotkeys“ zu definieren. Wenn Sie diese Tasten zum Aktivieren der Bedieneinheit drücken, „springt“ die Anzeige sofort in das gewünschte Menü.

Die Tasten eine Sekunde gedrückt halten oder nach Aktivierung erneut drücken.

### 3.2.7 Optionale Funktionen ab Version LP/LQ14

#### Vorsicht

Mit Version LP/LQ14 wurde auch die Hardware der Tastaturplatine von FlatControl geändert. Diese Firmwareversion ist nicht abwärtskompatibel zu früher verwendeter Hardware. Verwenden Sie nur Hardware, die mit dieser Firmware kompatibel ist. Eigenmächtige Umbauten und Änderungen sind verboten.

Folgen der Änderung der FlatControl Tastaturplatine:

- Umstellung auf blaues Display
- Sichtschutz bei allen VdS-Versionen
- bessere Lesbarkeit
- geringerer Stromverbrauch
- neue Echtzeituhr
- Uhrzeit- und Datumserhalt von bis zu 25 Tagen (bisher 7) bei Spannungsfreiheit

Die Firmwareversion der Bedieneinheit können Sie via Menü Status / Info anzeigen. Siehe Seite 76. Einige Funktionen können mit der optionalen PC-Software TwinComm programmiert werden.

Schlösser zurücksetzen

Die Schlossadressen 0,1,2 und 3 können via Menü / Hotkey auf „0“ gesetzt werden.

VdS-Versionen 2 und 3 in einer Software

Auswahl beim Installationsprozess. Danach Versionsabfrage der Schlossriegel.

Hotkeys

Neuer Hotkey „Reset des Vorgangszählers“ und geänderte Reihenfolge der Vorbereitung ab Werk.

Spezieller Zutritt über TwinComm konfigurierbar

Auch via TwinComm ist ‚Spezieller Zutritt‘ konfigurierbar. Durch die Definition eines Öffnungszeitraums oder / und eine Höchstanzahl an Öffnungen kann so die Öffnungsberechtigung von Benutzern eingeschränkt werden.

Automatisches Kopieren Managercode

Dieser Code wird beim Ändern automatisch von Schloss 1 auf Schloss 2 kopiert.

Anzeige Rückcode

Der Rückcode wird nur bei geschlossenem Zustand und Riegelwerk (Schalter) angezeigt. Bei offenem Zustand werden statt des Rückcodes 4 Sternchen angezeigt.

Anzeige Seriennummer

Die Seriennummer wird immer bei Neustart und erneuter Bestromung angezeigt.

Benutzergruppenbeschränkung auch während Freigabezeit

Die Benutzergruppenbeschränkung greift auch in der Freigabezeit nach einer Öffnungsverzögerung.

Menüs „Abmelden“: Transfer von PIN-Code und Codekarte

In den Menüs „PIN-Code/Abmelden“ und „Karte/Abmelden“ kann das Löschen des Codes / der Karte auf weitere Schlösser übertragen werden.

Abhängige Einmalcodes via TwinComm

Via TwinComm kann konfiguriert werden, dass jeder via Benutzermatrix berechtigte Benutzer mit Einmalcode öffnen muss.

Benutzer öffnen mit Einmalcode

Lokal (via Benutzermatrix) kann für Benutzer individuell eingestellt werden, ob sie mit 6-stelligem Einmalcode öffnen können sollen (nur mit Firmware Version 14). Wenn für Benutzer gewählt, müssen diese abhängig von den Systemeinstellungen zum Öffnen in der genannten Reihenfolge eingeben:

Benutzer- / Personalnummer -> PIN-Code und / oder Chipkarte -> Einmalcode oder RFID-Tag -> Einmalcode.

Protokollierung der Eingabe von abhängigem Einmalcode

Die Eingabe von abhängigem Einmalcode wird separat protokolliert.

Codealterung(Ablauf Gültigkeit vonCodes)

Jahres-, Benutzungs-, Programmierungs-Codealterung

Zusätzlich kann für die Codealterung via TwinComm eingestellt werden, ob die PIN-Codes jährlich zum 01.01. geändert werden müssen (=Jahres-Codealterung), ob die Alterung ab der jeweils zuletzt ausgeführten Bedienungsaktion „läuft“ (Benutzungs-Codealterung) oder ob sie jeweils ab dem Zeitpunkt der letzten PIN-Code-Änderung (Programmierung) gilt.

## 4 Bedienung

Mit der Bedieneinheit FlatControl in der Version für das jeweilige System können Sie Systeme TwinLock Business einstellen und bedienen.

### 4.1 Bedienelemente Bedieneinheit FlatControl

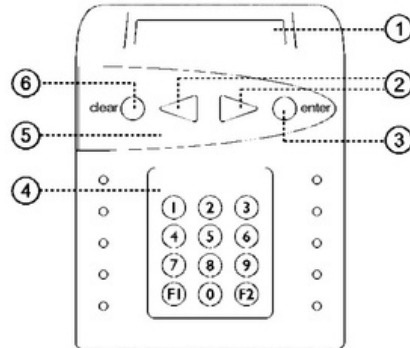


Abb. 18: Bedienelemente der Bedieneinheit FlatControl

- 1) Display
- 2) Menütasten < und > zur Navigation
- 3) Enter-Taste zum Bestätigen von Menü-Auswahl und Eingabewerten
- 4) Tastenfeld mit Ziffern- und Funktionstasten
- 5) Menütastatur
- 6) Clear-Taste zum Abbrechen

Ein Einschub für kontaktbehaftete Chipkarten ist unten an der Bedieneinheit.

Abhängig von der Systemvariante erfolgt die Codeeingabe über die Ziffern- oder über die Menütasten einschließlich Clear und Enter.

Eine Buchse zum Anschluss des Kabels für die Notstromversorgung befindet sich an der Unterseite der Bedieneinheit.

Die Anzeige beginnt nach einigen Sekunden zu blinken, nach einigen weiteren Sekunden ohne Eingabe wird sie automatisch ausgeschaltet.

Aktivieren Sie die Anzeige durch Drücken einer beliebigen Taste.

## 4.2 Hotkeys

Zusätzlich zur Navigation über die Menüs des Displays der Bedieneinheit können Sie mit einem der optionalen Softwareprogramme beliebige Tasten von 0-9 sowie F1 und F2 als Hotkeys definieren.

Wenn Sie diese Tasten gleich nach dem Aktivieren der Bedieneinheit drücken, „springt“ die Anzeige sofort in das gewünschte, definierte Menü. Die dafür normalerweise erforderliche Navigation wird überflüssig.



Abb. 19: Definition von Hotkeys(Beispiele)

Falls das System so eingestellt ist, dass auch die Code-Eingabe über die Zifferntasten erfolgt, ist dies wie bisher möglich. Das System stellt die Funktion der Tasten zum richtigen Zeitpunkt automatisch um.

## 4.3 Konfiguration mit PC Software TwinComm

Das System ist ohne zusätzliche Software funktionsfähig. Mit PC Software TwinComm sind zusätzliche Optionen verfügbar. PC Software vereinfacht die Konfiguration, ermöglicht das Auslesen des Ereignisprotokolls und die Programmierung von Zeitprogrammen. Zusätzlich kann die Autorisierung für Benutzer flexibel angepasst werden.

Der Systemverwalter gibt die für die Konfiguration erforderlichen Daten über die grafische Benutzeroberfläche der Software ein.

Der Datenaustausch mit System TwinLock erfolgt über ein optionales Kartenlese- /

Schreibgerät, am PC, mit Chipkarte TwinCard configuration II und der Servicefunktion Import / Export an der Bedieneinheit.

## 4.4 Betrieb mit abhängigen Einmalcodes

Der Betrieb mit abhängigen Einmalcodes ist nur möglich, wenn die unten aufgeführten Voraussetzungen erfüllt sind. Benutzer geben nach ihrer Benutzer- oder Personalnummer und nach PIN-Code oder Code-Karte / RFID Karte zusätzlich noch abhängigen Einmalcode ein. Die Einmalcodes werden mit optionaler Code-Generierungs-Software generiert.

Beim Schließen nach einem Öffnen mit Einmalcode wird ein vierstelliger Rückcode WTU-Code: XXXX auf dem Display der Bedieneinheit angezeigt, der beispielsweise telefonisch zurückgemeldet und vom zuständigen Mitarbeiter zum Abschließen des

Vorgangs verwendet werden kann.

Der jeweils letzte Rückcode kann auch mit Menü Status / Info angezeigt werden.

### 4.4.1 Voraussetzungen für abhängigen Einmalcode

- Produktversion TwinLock B7X0 / C8X0 / D9X0 Business LS
- Person an Schloss angemeldet (PIN und / oder Karte dort gespeichert)
- In Code-Generierungs-Software / Benutzermatrix (PC-Software) ist die Berechtigung Einmalcode für die Person aktiviert
- Aktivierungscode (7-stellig) ist konfiguriert
- Modus / WTU-Funktion ist auf Wert „0“ oder „1“ gesetzt
- Datum und Uhrzeit sind korrekt und synchron
- Schloss ist korrekt ausgewählt
- Firmware Version LP/LQ14

## 4.5 Systemstatus

Systemeinstellungen sind nur bei geöffnetem System möglich.

Bei gesichertem System werden auf dem Display von FlatControl nur die Menüs **Oeffnen**, **Schliessen**, **Status / Info** und **Import / Export** angezeigt.

Um das System zu entsperren

- öffnen Sie Schloss 1, wenn Option „Zwangsfolge“ (ZF) nicht aktiv ist oder
- öffnen Sie alle Schlösser, wenn Option „Zwangsfolge“ aktiviert ist.

Wenn Option „Zwangsfolge“ aktiviert ist, können Benutzer bei Systemen mit 2 oder 3 Schlössern nicht auswählen, welches Schloss sie öffnen oder schließen wollen. Siehe auch das Glossar.

Mögliche Zustände des Systems:

Ungesichert Schloss 1 / alle Schlösser offen (ohne Zwangsfolge [ZF]), Anzeige aller Menüs, Einstellungen sind änderbar.

Teilgesichert mindestens ein Schloss offen und ein Schloss (Schloss 1) geschlossen, Systemeinstellungen sind nicht änderbar (nur ohne ZF)

Gesichert Schloss 1 / alle Schlösser geschlossen, Menü-Anzeige eingeschränkt, Öffnungs- und Notfall-Funktionen sind ausführbar, Systemeinstellungen sind nicht änderbar.

Der Systemstatus ist abhängig davon, ob Option „Zwangsfolge“ aktiviert ist oder nicht:

Systemstatus mit deaktivierter Option „Zwangsfolge“

Ungesichert / entsperrt, wenn Schloss 1 offen ist. Anzeige aller Menüs.

Teilgesichert gibt es in diesem Fall nicht.

Gesichert, wenn Schloss 1 verschlossen ist. Menüanzeige eingeschränkt.

Systemstatus mit aktivierter Option „Zwangsfolge“

Ungesichert / entsperrt, wenn alle Schlösser offen sind.

Teilgesichert, wenn mind. ein Schloss geschlossen und eines offen ist.

Gesichert, wenn alle Schlösser geschlossen sind.

Zustandskontakt von TwinXT (II) / TwinXT small / TwinAlarm

Nur bei Systemen mit TwinXT (II) / TwinXT small / TwinAlarm: Kontakt in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

Systemsignal von Zustandskontakt von TwinXT (II, small) / TwinAlarm

Nur bei Systemen mit TwinXT (II) / TwinXT small / TwinAlarm: Signal in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

## 4.6 Benutzer- / Personalnummern

Das System kann mit via Benutzermatrix der PC-Software (mit FLC Firmware ab Version LP09) so umgestellt werden, dass Personen statt systemspezifischen Benutzer- nummern ihre gewohnten Personalnummern eingeben können.

Wenn alle Personen am Schloss ihre Personal- statt ihrer Benutzernummern eingeben sollen:

1) Markieren Sie Kontrollkästchen „Personalnummer“.

2) Geben Sie in Spalte „Personalnummer“ die Pers.-Nummern der Benutzer ein.

Wenn alle Personen am Schloss ihre Benutzernummer eingeben sollen:

- Entfernen Sie gegebenenfalls die Markierung in Kontrollkästchen „Personalnummer“.

Achtung:

Personalnummern (für alle Benutzer, auch Master) können nur mit Karte TwinLock configuration II übertragen werden. Personalnummern dürfen keine führenden Nullen enthalten. Sie können ein- bis sechsstellig sein.

Es findet keine interne Protokollierung darüber statt, welche Art von Nummern von den Personen zu verwenden ist. Die Umstellung gilt auch für die Schlossmaster.

Auch nach der Umstellung auf Personalnummern werden auf dem Display der Bedieneinheit in den Menüs „Benutzer-Anzeige“ und „PIN-Code löschen“ Benutzernummern angezeigt.

### 4.6.1 Benutzer- / Personalnummereingeben

Systeme VdS Klasse 3: Nummern-Eingabe mit Menütasten

Systeme VdS Klasse 2: Nummern-Eingabe konfigurierbar  
(mit Menü- oder Zifferntasten)

Vorbedingungen Für Sie ist Kästchen Freigabe in der Benutzermatrix (TwinComm) markiert.

1. Führen Sie die Schritte einer Anleitung aus, bis die Identifizierung erforderlich ist.

*Das Display zeigt Code-Eingabe | Master. Wenn Sie nicht sicher sind, mit welchen Tasten Nummern einzugeben sind, probieren Sie es aus. Falls die Eingabe über Menütasten eingestellt ist, können Nummern alternativ auch mit Zifferntasten eingegeben werden.*

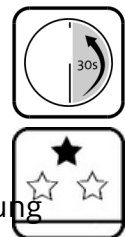
2. Wählen Sie mit < und > jeweils eine Ziffer der Nummer und Taste Enter oder geben Sie die Ziffern über die Zifferntasten ein. Schließen Sie die Eingabe der Personalnummer gegebenenfalls mit ENTER ab.

*Das Display zeigt jede eingegebene Ziffer, z.B. BenutzerNr.:02*

*Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie beispielsweise Code-Eingabe oder Bitte warten.*

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben die Benutzer- / Personalnummer erfolgreich eingegeben.



## 4.7 Benutzergruppen

Die an den Schlössern gespeicherten Personen / Benutzer eines jeden Systems können in zwei Gruppen eingeteilt werden:

Der Systemmanager aktiviert Option „Benutzergruppen“ im Menü der.

Der Schlossmaster meldet PIN-Code für Benutzer 99 an.

Ab Werk ist für TwinComm eingestellt, dass Benutzergruppe 1 die Benutzer Nr. 01 bis Nr. 49 umfasst und Benutzergruppe 2 mit Benutzer Nr. 50 beginnt und mit Nr. 100 endet. Mit dieser Software kann die Gruppengröße angepasst werden

(Twin-Comm: Einstellungen / 2. Benutzergruppe).

Der Schlossmaster verwaltet die Benutzer der ersten Gruppe, der Benutzer 99,

der

4.7.1 Einstellung Bedienung mit „Benutzergruppen“ aktiviert  
 4.7.1 Bedienung mit „Benutzergruppen“ aktiviert  
 der zweiten Gruppe.

### Vorsicht

Ohne autorisierten WTU-Master mit angemeldetem Code kann der WTU-Benutzerbereich nicht verwaltet werden. Statten Sie Benutzer 99 vor der Wahl von ‚Benutzergruppen‘ mit allen erforderlichen Rechten aus (siehe Abschnitt „Benutzer autorisieren“) und melden Sie Code für ihn am Schloss an.

Für Benutzer ändert sich die Bedienung mit „Benutzergruppen“ (Benutzergruppe Bank / Benutzergruppe WTU, Werttransportunternehmen) bis Version LP/LQ05 nicht.

Ab Version LP/LQ05 kann über Feld „Öffnung (Benutzergruppen, zwingend)“ auf Registerkarte „Einstellungen“ von TwinComm ausgewählt werden, ob die Gruppenmitglieder bei „4-Augen-Prinzip (Öffnung)“ oder „Parallelcode“

- nur gemeinsam mit Mitgliedern ihrer Gruppe (Wert: „gleich“) oder
- nur mit einem Mitglied der anderen Gruppe (Wert: „verschieden“) oder
- mit einer Person einer beliebigen Gruppe (Wert: „keine“) öffnen können.

Bei der Wahl von ‚Benutzergruppen‘ (siehe „Zwei ‚Benutzergruppen‘ wählen“ in diesem Kapitel) werden die Benutzer jedes Schlosses in zwei Gruppen eingeteilt. Die Gruppengröße wird via PC-Software definiert (ab Werk Benutzer 01-50 bei Schlossmaster und Benutzer 51-98 bei WTU-Master).

Der Schlossmaster verwaltet die erste Gruppe (Benutzer 01 bis XX-1). Benutzer 99, der zum WTU-Master wird, verwaltet die WTU-Benutzer (Benutzer XX bis 98).

## 4.7.2 Master / WTU-Master wählen

Schloss- und WTU-Master wählenvor ihrer Code-Eingabe zusätzlich „Master“ beziehungsweise „WTU-Master“:

1. Führen Sie als Master / WTU-Master die Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.  
*Vor jeder Master- oder WTU-Mastercode-Eingabe zeigt das Display bei aktiver WTU-Funktion: Code-Eingabe | Benutzer: Master und springt nicht weiter zur Code-Eingabe.*
2. Bestätigen Sie **Master** mit **Enter** oder wählen Sie mit den Menütasten **<** und **>** **WTU-Master** und **Enter**.  
*Das Display zeigt **WTU-Master** oder **Master**, **Code-Eingabe**, gegebenenfalls **0123456789** und **Code**.*
3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben erfolgreich Master / WTU-Master gewählt.

## 4.8 Benutzer autorisieren

Vor der Code-Eingabe geben Benutzer ihre Benutzer- oder Personalnummer (Pers.-Nr.) ein.

Der Systemverwalter definiert die Autorisierung von Benutzern via TwinComm in einer Matrix, indem er für Benutzer Kontrollkästchen aktiviert (Beschreibung der Kontrollkästchen siehe unten). Diese Autorisierung ist fest eingestellt. Mit der optionalen PC-Software ist sie auch änderbar.

Damit diese Berechtigungen im Schlosssystem gelten, importiert der Systemverwalter die Konfiguration aus der PC-Software in das System TwinLock Business.

Damit ein Benutzer ein Schloss öffnen kann, muss der Schlossmaster (Inhaber des Mastercodes dieses Schlosses) für den Benutzer außerdem

- PIN-Code und optional auch
- Codekarte (Chip- /RFID Karte)

am Schloss angemeldet haben.

Wenn für Benutzer das Kästchen Freigabe in der Benutzermatrix nicht markiert ist, haben die Benutzer keine Rechte und sind für alle Funktionen gesperrt.

Autorisierung zum Öffnen eines Schlosses mit PIN-Code:

Der Systemmanager aktiviert für den Benutzer die Kontrollkästchen PIN-Code, Freigabe und Öffnen, mit Einbruchmeldeanlage auch Unscharf.

Autorisierung zum Öffnen eines Schlosses mit PIN-Code und Codekarte:

Der Systemmanager aktiviert für den Benutzer alle oben aufgeführten Kästchen und zusätzlich Chipkarte.

Autorisierung zur Öffnung eines Schlosses mit PIN-Code und RFID:

Der Systemmanager aktiviert für den Benutzer die Kästchen Karte, Freigabe, PIN-Code und Öffnen. Zusätzlich muss via TwinComm, Seite „Einstellungen“, der Wert „RFID“ für Parameter „Codekarte“ gesetzt und das entsprechende RFID-System gewählt sein.

## 4.8.1 Felder und Kontrollkästchen der Benutzermatrix

Die Benutzermatrix kann via PC-Software angezeigt und gegebenenfalls auch bearbeitet werden.

### Vorsicht

Benutzer können kein Schloss öffnen, wenn sie nicht ausreichend autorisiert sind.

Deaktivieren Sie ab Werk aktivierte Kontrollkästchen in der Benutzermatrix nur, wenn Sie dieses Handbuch gelesen haben und, falls erforderlich, nach Beratung durch eine Fachkraft für das System. Aktivieren Sie bei Bedarf weitere Kontrollkästchen wie „Chipkarte“.

Damit ein Benutzer bestimmte Bedienvorgänge ausführen kann, müssen ihm alle dafür nötigen Berechtigungen verliehen werden.

Benutzer und Schlossmaster (=Benutzer 00) können vom Systemmanager, der selbst nicht öffnen kann, zur Öffnung von Schlössern autorisiert werden.

### Hinweis

Zusätzlich zur Benutzer-Autorisierung kann der Systemmanager zwei Benutzergruppen in Bereich „Einstellungen“ der PC-Software definieren und für diese Öffnungsbedingungen festlegen. Siehe Abschnitt „Bedienung bei aktivierter WTU-Funktion“ unten in diesem Kapitel.

Es folgt eine Liste aller Kontrollkästchen, die es in der Benutzermatrix gibt. Der Systemmanager kann bestimmte Berechtigungen ändern. Der Systemmanager kann Kästchen für Benutzer markieren oder nicht.

### Felder und Kontrollkästchen

#### Benutzer

	Laufende Benutzernummer, nicht änderbar. Ab Werk wird der Benutzer mit dieser Nummer identifiziert.
Name	Beschreibbares Feld für den Namen des Benutzers; Eintrag hier wird in Protokoll übernommen.
PIN-Code	Berechtigung zur Eingabe von PIN-Code.
Karte	Berechtigung zu Code-/Daten-Eingabe via Karte (RFID-/Chipkarte).
Fingerprint	nur bei biometrischen Systemen: Berechtigung zur Eingabe biometrischer Daten.
1 aus 3	Berechtigung, eine Art der Authentifizierung wählen zu können (PIN-Code, Chipkarte oder ggf. Fingerprint).
2 aus 3	Berechtigung, zwei Arten der Authentifizierung aus den drei möglichen Arten auswählen zu können (nur mit BioPIN).
Schnellöffnung	Berechtigung, Schlösser trotz aktiver Zeitprogramme wie Wochenprogramme oder Sperrzeit zu öffnen.
Freigabe	allgemeine Freigabe zur Bedienung des Systems.
Öffnen	Berechtigung zum Schloss-Öffnen.
Schließen	Anforderung, das Schloss mit Code zu schließen.
Service	Berechtigung, die Konfiguration zu importieren / Wochenprogramme zuzuweisen.
2-Augen	Berechtigung, trotz gesetztem 4-Augen-Prinzip / Parallelcode allein öffnen / schließen zu dürfen.

### Vorsicht

Bei Systemen mit Einbruchmeldeanlage kann ein Benutzer (auch Schlossmaster) ein Schloss nur öffnen, wenn er zum Unscharf Schalten befugt ist.  
Entfernen Sie die Markierung aus Kästchen Unscharf nicht für Benutzer, die Schlösser öffnen sollen.

Unscharf	Berechtigung zum Unscharf Schalten einer externen Einbruchmeldeanlage.
WP1 – WP5	Wenn markiert, gelten die Wochenprogramme für Benutzer und diese dürfen nur während der für die Wochentage definierten Zeiträume öffnen.
Einmalcode	Optionale Zuordnung der Verwendung von abhängigem Einmalcode.
Personalnummer	Ab Version LP09: Feld zur Eingabe einer ein- bis sechsstelligen Personalnummer. Nur wenn das Kästchen ‚Personalnummer‘ oben in der Benutzermatrix markiert ist, gaben alle Benutzer ihre Personalnummer statt ihrer Benutzernummer ein, bevor Sie Schlösser öffnen.
Templatename	keine Berechtigung, optional, gegebenenfalls Anzeige des Namens von Benutzern zugeordneten Templates (falls Templates nach Zuordnung nicht gelöscht oder umbenannt wurden)
Folgende Option ist für TwinLock Business hier nicht einstellbar (Stand 09/2023):	
No-return-code	Optionale Zuordnung von Code, mit dem Benutzer einmal öffnen kann und dann nur immer dann, wenn zuvor ein anderer Benutzer geöffnet hat.

## 4.8.2 Werkseinstellung Rechte Benutzermatrix

Benutzercodes sind ab Werk nicht programmiert.

Managercode (Nr.225):	PIN-Code   Freigabe   Service (nicht änderbar) PIN-Code   Chipkarte   Fingerprint   1 aus 3   Schnellöffnung   Freigabe   Öffnen   Schließen   Service
Master (Nr.00):	2- Augen   Unscharf
Benutzer (Nr.01-99):	keine (programmierbar)

### 4.8.3 Berechtigungen Manager / Master / Benutzer

Übersicht der Berechtigungen von Manager (Nr.225) Master (Nr.00), Benutzer (Nr.01-99) und gegebenenfalls von WTU-Master / Master Gruppe 2 (Nr.99). Beschreibung der Werkseinstellung, via Benutzermatrix teilweise änderbar.

- Manager** (Nr.225): eigenen Code ändern, Systemzeit setzen  
Codes und Karte von Master verwalten,  
gegebenenfalls WTU-Service- und Servicecode verwalten,  
WTU-Funktion wählen,  
Stand des Vorgangszählers prüfen und setzen,  
Konfiguration im- und exportieren, Protokoll exportieren,  
Benutzergruppen definieren,  
Schlösser anmelden, Reset  
Lizenz Einstellungen ändern,  
Alarmgeräte ein- und ausschalten
- Optional: Codeverknüpfung, Parallelcode, Zwangsfolge wählen,  
Zeitverzögerung pro Schloss / Wochenprogramm setzen,  
Wochenprogramme definieren,
- Master** (Nr.00): eigenen Code ändern,  
Codes und Karten von Schlossbenutzern verwalten,  
Schlösser öffnen und schließen, gegebenenfalls Einbruch-  
meldeanlage (EMA) un- / scharf schalten),  
Motorservice, 1x Riegelwerk ignorieren, Neustart,  
Sprache wählen und importieren,  
Konfiguration im- und exportieren, Protokoll exportieren
- WTU-Master** (Nr.99) /  
Master Gruppe 2  
(optional): eigenen Code ändern,  
Codes und Karten für Schlossbenutzer Nr.XX-98 verwalten,  
Schlösser öffnen und schließen, gegebenenfalls Einbruch-  
meldeanlage (EMA) un- / scharf schalten,  
Motorservice, 1x Riegelwerk ignorieren, Neustart,  
Sprache wählen und importieren,  
Konfiguration im- und exportieren, Protokoll exportieren
- Benutzer** (Nr.01-98/99): eigenen Code ändern,  
Schlösser öffnen und schließen,  
gegebenenfalls EMA un- / scharf schalten,  
1x Riegelwerk ignorieren, Neustart,  
Sprache wählen und importieren,  
Konfiguration (Import optional) und Protokoll exportieren

## 4.9 Menüführung in der Bedieneinheit

### 4.9.1 TwinLock BC7X0 Business (mit FlatControl, bei geöffnetem System)

```

Systemmenü mit Anzeige Mo 11.09.23 8:35
Oeffnen
Schliessen
Status / Info
Einstellungen
├── Mastercodes
├── Managercode
├── PIN-Code
│   ├── Anmelden Abmelden
│   ├── Benutzer-Anzeige
│   └── 
├── Codekarte
│   ├── Anmelden Abmelden
│   ├── Benutzer-Anzeige
│   └── 
├── Schlosssystem(Version LP/LQ11 und höher)
│   ├── Codeverknüpfung
│   │   ├── Öffnen
│   │   ├── Konfiguration
│   │   └── Freigabezeit
│   ├── Parallelcode
│   ├── Zwangsfolge
│   ├── Zeitverzögerung
│   │   ├── Schloss
│   │   └── Wochenprogramme
│   └── Wochenprogramm
├── Datum/Uhrzeit
├── Alarmgeräte
├── Service
├── WTU-Funktion
├── 
├── Reset (für neuen Setup des Systems)
│   ├── Terminal
│   └── Schloss
├── Motor Service
├── Schloss anmelden
├── 1x Riegelwerk
├── Lizenzierung
├── Import/Export
├── Konfiguration
└── Sprache
  
```

## 4.10 PIN-Codes

### Vorsicht

---

Geben Sie Code nur in einer sicheren Umgebung ein.

Mit werksseitigen Systemmanager- und Mastercodes ist das System nicht gesichert.

Gefahr der unberechtigten Öffnung.

Ändern Sie werksseitige Codes aus Sicherheitsgründen sofort nach der Installation.

---

Einfache Codes (z.B. 123456) und Codes mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

---

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

---

Der Mastercode kann gelöscht werden.

Gefahr von Funktionsverlust.

Löschen Sie den Mastercode nicht. Falls erforderlich, kann der Manager den Master neu autorisieren.

---

#### 4.10.1 Arten und Anzahl von PIN-Codes in jedem Schloss

- 1 Managercode (ohne Berechtigung zur Öffnung des Schlosses)
- 1 Mastercode (mit optionaler Berechtigung zur Öffnung des Schlosses)
- 1 optionaler WTU-Mastercode  
(mit optionaler Berechtigung zur Öffnung des Schlosses)
- 1-99 PIN-Codes für Benutzer (mit optionaler Berechtigung zur Öffnung des Schlosses, siehe auch Abschnitt „Benutzer-Autorisierung“)

Mit dem Managercode des Schlosses Nr.1 kann das gesamte System konfiguriert werden. Deshalb wird er als Systemmanagercode, kurz als Systemcode, bezeichnet und sein Inhaber als Systemmanager.

Mit dem Mastercode jedes Schlosses können die Benutzercodes des Schlosses an- und abgemeldet werden. Sein Inhaber wird als Schlossmaster bezeichnet. Er kann vom Systemmanager optional zur Schloss-Öffnung autorisiert werden. Manager- und Mastercodes können nicht abgemeldet oder deaktiviert werden. Mit dem optionalen WTU-Mastercode wird gegebenenfalls die 2. Benutzergruppe verwaltet.

Mit jedem vom Schlossmaster am Schloss angemeldeten PIN-Code für Benutzer kann das Schloss geöffnet werden, wenn der Benutzer vom Systemmanager autorisiert wurde.

PIN-Codes für Benutzer sind werksseitig nicht vorprogrammiert. Über die Benutzer-

matrix der PC-Software ist definiert, zu welchen Aktionen sie berechtigen. Sie können vom Schlossmaster an- und abgemeldet werden. Abhängig von ihrer Autorisierung können Benutzer gegebenenfalls ihren Code ändern.

Die Anzahl der Ziffern im PIN-Code (für Benutzer-, Master-, Manager- und Systemmanager) ist abhängig von der VdS-Klasse des Systems.

Die VdS-Klasse kann in Menü Status / Info auf dem Display der Bedieneinheit angezeigt werden.

Systeme der VdS-Klasse 2 enthalten ausschließlich Schlösser des Typs VdS2, solche der Klasse 3 Schlösser des Typs VdS 3. Ebenso bei Systemen der VdS-Klasse 4.

Bei Systemen der VdS-Klasse 3 und 4 ist jeder PIN-Code achtstellig.

Bei Systemen der VdS-Klasse 2 ist jeder PIN-Code sechsstellig.

Master- und Systemmanagercodes ab Werk		
	Master	System / Manager
VdS Klasse 2	123456 (Benutzer 00)	111111 (Benutzer 225)
VdS Klasse 2 optional	12345600 (Benutzer 00)	11111100 (Benutzer 225)
VdS Klasse 3/4	12345678 (Benutzer 00)	11111111 (Benutzer 225)

## 4.10.2 PIN-Code eingeben

Mit welchen Tasten die Benutzer an der Bedieneinheit ihre persönliche PIN oder ihren PIN-Code eingeben können, ist abhängig von der Art der Konfiguration:

Bei VdS Klassen 3 / C und 4 / D nur mit Menütasten.

Bei VdS Klasse 2 / B Schlössern optional mit Zifferntasten oder mit Menütasten (via PC-Software einstellbar).

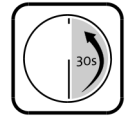
Einmalcode (OTC): nur mit Zifferntasten.

### 4.10.2.1 PIN-Code mit Menütaste eingeben

Systeme der VdS Klasse 3: Code-Eingabe mit Menütasten.

Systeme der VdS Klasse 2: Code-Eingabe mit Menütasten optional.

Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen. Ihr PIN-Code ist am Schloss angemeldet.



1. Führen Sie die Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.

*Das Display zeigt vorder Code-Eingabe unter anderem 0123456789. Der Cursor steht bei einer beliebigen Ziffer.*

2. Wählen Sie mit < und > jeweils eine Ziffer des Codes und bestätigen Sie jeweils mit Enter.

*Das Display zeigt für jede eingegebene Ziffer ein Sternchen (Asterisk): Code: \*\*\*. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie beispielsweise Bitte warten.*

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben den PIN-Code erfolgreich eingegeben.

### 4.10.2.2 PIN-Code mit Zifferntaste eingeben

Systeme der VdS Klasse 2, ab Werk Code-Eingabe mit Zifferntasten.

Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen. Ihr PIN-Code ist am Schloss angemeldet.

1. Führen Sie Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.

*Das Display zeigt vorder Code-Eingabe nicht 0123456789, sondern unter anderem Benutzer Nr. | Code:. Der Cursor steht an der Stelle für die erste Ziffer. Daran ist erkennbar, dass der Code mit den Zifferntasten einzugeben ist.*



2. Wählen Sie die Ziffern des Codes mit den Zifferntasten.

*Das Display zeigt für jede eingegebene Ziffer ein Sternchen (Asterisk): Code: \*\*\*. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie beispielsweise Bitte warten.*

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben den PIN-Code erfolgreich eingegeben.

## 4.11 RFID Karten und Chipkarten

### Vorsicht

Gefahr des Verlustes von Daten / Karten.  
Beachten Sie die Sicherheitsrichtlinien und bewahren Sie Karten stets an Orten auf, zu denen nur Sie Zugang haben. Tun Sie dies so, dass die Daten geschützt sind (RFID-Karten: Alufolie oder geeignete Schutzhüllen, Scrambler-Karten).

Scrambler-Karte: NFC Karte, die RFID-Karten in der Nähe gegen Auslesen schützt: Durch erzeugte Störungen wird ein Leser gezwungen, die Kommunikation zu beenden, bevor sensible Daten übertragen werden können.

Die Chipkarten TwinCard können in Kombination mit PIN-Code zur Schloss-Öffnung, zur System-Konfiguration, zum Anzeigen des Protokolls und zum Import von Sprachen verwendet werden. Siehe auch Abschnitte „Chipkarten TwinCard“ auf Seite 22 und „Chipkarte in FlatControl / in Leser einlegen“.

### 4.11.1 RFID Karten

Optionale RFID Karten können nur vom Systemmaster angemeldet werden. Pro Schloss kann für bis zu 99 Benutzer je eine RFID Karte mit oder ohne Benutzercode am Schloss an- und abgemeldet werden. Werksseitig sind die Kartencodes für die Benutzer 01 – 99 inaktiv. Siehe auch Abschnitt „Benutzer autorisieren“. RFID Karten können via Kartenleser angemeldet werden.

Über TwinComm kann die Art der Codekarte beispielsweise auf Mifare eingestellt werden, womit die RFID Karte zur Codekarte gemacht werden kann. Auf einer RFID Karte können die Personalnummer oder die persönliche PIN oder diese beiden Nummern zusammen gespeichert werden.

#### 4.11.2 RFID Karte mit Bedieneinheit einlesen

Für dieses System gibt es unterschiedliche Arten von RFID Karten.

Siehe auch „RFID Karten“ auf Seite 48. Via RFID Karte können die Personalnummer oder die persönliche PIN (für die Eingabe von flexiblem Einmalcode) oder diese beiden Nummern zusammen gespeichert übermittelt werden.



Vorbedingungen - Sie sind zum Öffnen auch mit Karte autorisiert.

- Der Systemmanager hat beispielsweise ‚Mifare‘ als Codekarte eingestellt.
- für Sie sind zum Öffnen in der Benutzermatrix (TwinComm) die Kästchen Karte, Freigabe und Öffnen aktiviert.

Sie benötigen - eine optionale Karte TwinCard RFID



Abb. 20: RFID-Karten und Kartenleser

1. Wenn das Display der Bedieneinheit Lese Daten anzeigt, halten Sie die Karte TwinCard RFID sehr nahe vor die Zifferntasten der Bedieneinheit. *Die Karte wird gelesen.* Warten Sie, bis das Display Bitte warten anzeigt und ein Piepen ertönt / bis Lese Daten nicht mehr angezeigt wird.
2. Entfernen Sie die RFID Karte.
- 3.

Sie haben die Karte erfolgreich eingelesen.

### 4.11.3 Codekarte TwinCard code access

Optionale Codekarten TwinCard code access können vom Schlossmaster angemeldet werden, für bis zu 99 Benutzer pro Schloss je eine Chipkarte mit PIN-Code. Werksseitig sind die Kartencodes für die Benutzer 01 – 99 inaktiv.

Siehe auch Abschnitt „Benutzer autorisieren“ auf Seite 40.

Wenn der Systemmanager einen Benutzer dazu autorisiert hat, kann dieser mit PIN-Code und der optionalen Chipkarte TwinCard code access ein Schloss öffnen.

Siehe Abschnitt „Zusätzlich mit Codekarte öffnen“ auf Seite 52.

### 4.11.4 Chipkarten TwinCard configuration II / - language

Mit der optionalen Chipkarte TwinCard configuration II können ausgewählte Benutzer (Kästchen Freigabe und Service in der Benutzermatrix markiert) gegebenenfalls das Protokoll exportieren. Der Systemmanager kann damit die Konfiguration importieren und exportieren.

Mit TwinCard language kann der Systemmanager Sprachen importieren.

Siehe auch Abschnitt „System einrichten“ auf Seite 60.

### 4.11.5 Chipkarte in FlatControl / in Leser einlegen

Sie benötigen eine optionale Chipkarte

1. Wenn das Display der Bedieneinheit **Karte ein** anzeigt, legen Sie die Chipkarte in den Kartenleser.

*Die Karte rastethörbar ein. Der Chip befindet sich in der oberen Kartenhälfte, die Kartenrückseite zeigt in Ihre Richtung.*



Abb. 21: Karte und Kartenfach FlatControl

- 1) Kartenfach der Eingabeeinheit FlatControl
  - 2) Chipkarte TwinCard (code access / configuration II / language)
2. Warten Sie, bis das Display **Karte aus** anzeigt.
  3. Entnehmen Sie die Chipkarte aus der Bedieneinheit.

Sie haben die Karte erfolgreich eingelegt und sie wieder entnommen.

## 4.12 Öffnen und Schließen

Je nach Konfiguration des Schlosssystems geben Benutzer vor der Code-Eingabe ihre Benutzer- oder ihre Personalnummer (Pers-Nr.) ein. In den folgenden Beschreibungen wird meist nur eine dieser Möglichkeiten beschrieben.

### Vorsicht

Wenn am Display „Neustart oder Stromlos“ angezeigt wird, könnte ein Manipulationsversuch stattgefunden haben. Unterziehen die Bedieneinheit einer Sichtprüfung auf Beschädigung. Wenn erforderlich, kontaktieren Sie eine Sicherheitskraft. Die Meldung wird nach Code-Eingabe und Öffnung nicht mehr angezeigt.

Bei Systemen mit Einbruchmeldeanlage (EMA) können Benutzer kein Schloss öffnen, wenn sie nicht zum Unscharf Schalten autorisiert sind.

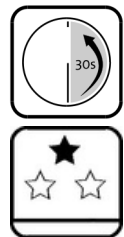
Wenn eine EMA angeschlossen ist, markieren Sie für Benutzer in der Benutzermatrix von PC-Software auch Kästchen Unscharf.

Um das System zu entsperren, öffnen Sie je nach Systemeinstellung alle Schlösser oder nur Schloss 1. Siehe auch Abschnitt „Systemstatus“. Abhängig von der Konfiguration kann zum Öffnen die Eingabe von Code und Karte von bis zu drei Benutzern erforderlich sein.

### 4.12.1 Schloss mit PIN-Code öffnen

Vorbedingungen: Kästchen PIN-Code und Freigabe 1 von 3 Öffnen und Unscharf sind in der Benutzermatrix für sie markiert. Der Master hat PIN-Code für Sie angemeldet.

- Drücken Sie kurz die Taste Clear, warten Sie etwas und drücken Sie Taste >, bis Öffnen angezeigt wird, und Taste Enter.  
*Das Display zeigt Öffnen und Code-Eingabe | Schloss 1.*
- Wählen Sie mit > gegebenenfalls das Schloss und Enter.  
*Das Display zeigt gegebenenfalls Code-Eingabe | Standard.*
- Bestätigen Sie gegebenenfalls Standard mit Taste Enter.  
*Das Display zeigt Code-Eingabe | Benutzer: Master.*
- Wählen Sie mit die Benutzer- / Personalnummer und gegebenenfalls Enter.  
*Siehe auch „Benutzer- / Personalnummer eingeben“ auf Seite 38.*  
*Das Display zeigt Code-Eingabe | Benutzer: 01 oder Code-Eingabe | Pers-Nr: XXXXXX und Benutzer / Pers-Nr: XXXXXX | PIN-Code.*
- Bestätigen Sie mit Enter.  
*Das Display zeigt Benutzer Nr / Pers-Nr: XXXXXX, gegebenenfalls 0123456789 und Code:.. Siehe auch „PIN-Code eingeben“ ab Seite 47.*  
*Das Display zeigt Code-Eingabe | Benutzer: XX.*
- Geben Sie Ihren PIN-Code ein.  
*Falls Eingabe einer weiteren Code-Art erforderlich, Codekarte wählen und diese Codeart eingeben.*  
*Bei Benutzern mit Authentifizierung nur mit PIN-Code wird Öffnen | Bitte warten angezeigt. Der Schlossriegel fährt ein. Das Display zeigt Öffnen | Schloss auf: Nr. und gegebenenfalls System entsperrt.*



Sie haben das Schloss erfolgreich geöffnet.

## 4.12.2 Zusätzlich mit Codekarte öffnen

**Vorbedingungen** Die Kästchen Karte, PIN-Code, Freigabe, (1 von 3), Öffnen und, falls erforderlich, Unschärf sind in der Benutzermatrix für sie markiert. Der Schlossmaster hat Ihre Codekarte am Schloss angemeldet.

Sie benötigen eine Chipkarte TwinCard code access / eine RFID-Karte.

1. Drücken Sie kurz die Taste Clear, warten Sie etwas und drücken Sie Taste >, bis Oeffnen angezeigt wird, und Taste Enter.

Das Display zeigt Oeffnen und Code-Eingabe | Schloss 1.

2. Wählen Sie mit > gegebenenfalls das Schloss und Enter.

Das Display zeigt gegebenenfalls Code-Eingabe | Standard.

3. Bestätigen Sie Standard mit Taste Enter.

Das Display zeigt Code-Eingabe | Benutzer: Master.

4. Wählen Sie mit die Benutzer- oder die Personalnummer und bestätigen Sie gegebenenfalls mit Enter.

Siehe auch „Benutzer- / Personalnummereingeben“ auf Seite 38.

Das Display zeigt beispielsweise Code-Eingabe | Benutzer: 01 und Benutzer Nr. | PIN-Code.

5. Wählen Sie mit > Karte und Enter.

Das Display zeigt Benutzer: XX | Karte ein.

Bei RFID-Karte zeigt das Display Lese Daten.

6. Legen Sie die Karte ins Kartenfach / Lesen Sie die RFID-Karte ein.

Siehe Seite 49 und Seite 50. Bei RFID-Karten öffnet das Schloss.

Das Display zeigt Bitte warten und bei Chipkarten Karte aus.

7. Entfernen Sie die Karte.

Die Eingabe einer weiteren Art von Code ist erforderlich. Falls noch nicht geschehen, wählen Sie PIN-Code und geben Sie diese Codeart ein. Siehe die Beschreibungen „Schloss mit PIN-Code öffnen“ oben.

Danach zeigt das Display

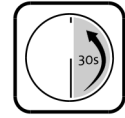
Oeffnen | Bitte warten. Der Riegel des Schlosses fährt ein. Das Display zeigt Oeffnen | Schloss auf: Nr.



Sie haben das Schloss erfolgreich geöffnet.

### 4.12.3 Beim Öffnen Stillen Alarm auslösen

Sokönnen Sieim Falleiner Bedrohung unauffällig Hilfeverständigen. Der Alarm kann nicht via Karte aktiviert werden. Bei PIN-Code wird er wie unten beschrieben aktiviert.



Vorbedingungen Option „Stiller Alarm“ ist via Software aktiviert. Weitere Vorbedingungen wie für „Schloss mit PIN-Code öffnen“ auf Seite 51.



Sie benötigen eine aktivierte Einheit TwinXT (II, small) / TwinAlarm und eine EMA.

1. Drücken Sie kurz die Taste Clear, warten Sie etwas und drücken Sie  $\>$ , bis **Oeffnen** angezeigt wird, und Taste Enter.  
*Das Display zeigt Code-Eingabe | Schloss 1.*
2. Wählen Sie mit  $\>$  und **Enter** gegebenenfalls das Schloss.  
*Das Display zeigtgegebenenfalls Code-Eingabe | Standard.*
3. Bestätigen Sie gegebenenfalls **Standard** mit Taste Enter.  
*Das Display zeigt Code-Eingabe |Benutzer: Master.*
4. Wählen Sie mit  $\>$  und Enter oder mit den Zifferntasten und Enter die Benutzernummer.  
*Das Display zeigt beispielsweise Code-Eingabe |Benutzer: 01 und Benutzer Nr. | PIN-Code.*
5. Bestätigen Sie Sie **PIN-Code** mit Taste Enter.  
*Das Display zeigt z.B. Benutzer XX, Code-Eingabe | Code:.*
6. Wählen Sie mit  $\<$  und  $\>$  alle Ziffern Ihres Codes außer der letzten. Bestätigen Sie jeweils mit **Enter**.
7. Wählen Sie mit  $\<$  und  $\>$  statt der letzten Ziffer (z.B. 8) deren Wert „+1“, also beispielsweise 9 und bestätigen Sie mit **Enter**.  
*Falls der letzte Wert eine 9 ist, geben Sie statt „10“ eine Null ein.  
Die Display-Anzeige und gegebenenfalls auch der weitere Öffnungsvorgang sind genau so wie bei einer „normalen“ Öffnung.*

Sie haben den Alarmcode eingegeben und erfolgreich Stillen Alarm ausgelöst.

#### 4.12.4 Schloss mit Codeverknüpfung öffnen

Nur wenn jeder der zwei beteiligten Benutzer alle ihm zugeteilten Arten der Authentifizierung durchführt, öffnet sich das Schloss.

Vorbedingungen Codeverknüpfung / „4-Augen-Prinzip (Öffnung)“ ist aktiviert worden. Weitere Vorbedingungen wie für „Schloss mit PIN-Code öffnen“ auf Seite 51.

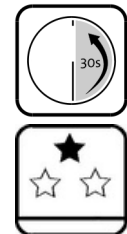


1. Drücken Sie kurz die Taste `Clear`, warten Sie etwas und drücken Sie Taste `>`, bis `Oeffnen` angezeigt wird, und Taste `Enter`.  
*Das Display zeigt Code-Eingabe | Schloss1.*
2. Wählen Sie mit `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt gegebenenfalls Code-Eingabe | Standard.*
3. Bestätigen Sie gegebenenfalls `Standard` mit Taste `Enter`.
4. Wählen Sie mit `>` oder mit den Zifferntasten und `Enter` Ihre Benutzernummer.
5. Wählen Sie je nach Ihrer Autorisierung mit `ENTERPIN-Code` oder mit `<` und `>` und `ENTER` Codekarte und führen Sie alle Schritte wie beim normalen Öffnen des Schlosses aus.  
*Siehe die Beschreibungen „Schloss mit ...öffnen“ am Anfang des Kapitels.  
Den nächsten Schritt führt eine zweite Person aus.  
Das Display zeigt Code-Eingabe &2 | Master.*
6. Ein zweiter Benutzer belegt seine Autorisierung am Schloss.  
*Das Display zeigt Oeffnen | Schloss auf: Nr.*

Gemeinsam mit einer zweiten Person haben Sie das Schloss erfolgreich mit Codeverknüpfung geöffnet.

#### 4.12.5 Schloss mit Öffnungsverzögerung öffnen

Vorbedingungen Als „Öffnungsverzögerung“ ist ein Wert größer Null eingestellt. Weitere Vorbedingungen wie für „Schloss mit PIN-Code öffnen“ auf Seite 51.



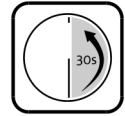
1. Drücken Sie kurz die Taste `Clear`, warten Sie etwas und drücken Sie Taste `>`, bis `Oeffnen` angezeigt wird, und Taste `Enter`.  
*Das Display zeigt Code-Eingabe | Schloss1.*
2. Wählen Sie mit `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt gegebenenfalls Code-Eingabe | Standard.*
3. Bestätigen Sie gegebenenfalls `Standard` mit Taste `Enter`.
4. Wählen Sie die Benutzernummer mit `>` oder mit den Zifferntasten und `Enter`.
5. Wählen Sie mit `Enter` `PIN-Code` und gegebenenfalls mit `>` und `Enter` `Codekarte` und öffnen Sie wie oben beschrieben.  
*Siehe die Beschreibungen „Schloss mit ...öffnen“ am Anfang des Kapitels.  
Das Display zeigt Oeffnen | Zeit: 00:00.*
6. Warten Sie, bis die Zeit der Öffnungsverzögerung abgelaufen ist.  
*Die Bedieneinheit piept 15x in kurzer Folge.  
Das Display zeigt Oeffnen | Schloss auf: Nr.*

Sie haben das Schloss erfolgreich geöffnet.

#### 4.12.6 Mit Öffnungsverzögerung und Freigabezeit öffnen

Diese Anleitung ist eine Weiterführung der vorhergehenden.

Vorbedingungen Siehe vorhergehenden Abschnitt. Zusätzlich ist Option 'Freigabezeit' in der PC-Software aktiviert.



1. Führen Sie Schritte 1-5 der vorhergehenden Handlungsanleitung aus und bereiten Sie sich darauf vor, eingeben zu können.

*Das Display zeigt Code-Eingabe | Benutzer: Master.*

*Ein akustisches Signal zeigt den Ablauf der Verzögerungszeit an. Während der folgenden Freigabezeit ertönt alle 2 Sekunden ein Signal.*



2. Wählen Sie gegebenenfalls mit > das Schloss und Enter.

*Das Display zeigt Code-Eingabe | Benutzer: Master.*

3. Wählen Sie mit > und Enter oder mit den Zifferntasten Ihre Benutzernummer.

4. Geben Sie Ihre(n) Code(s) ein.

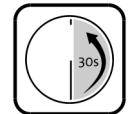
*Siehe Schritt 6 der vorhergehenden Anleitung. Ein akustisches Signal ertönt wiederholt. Das Display zeigt Öffnen | Schloss auf: 1.*

Sie haben das Schloss erfolgreich geöffnet.

#### 4.12.7 Schlösser mit Parallelcode öffnen

Ein Benutzer öffnet Schloss 1, ein zweiter Schloss 2 und ein dritter gegebenenfalls Schloss 3. Alle öffnen dabei gemäß ihrer Autorisierung.

Vorbedingungen Option „Parallelcode“ (nur für Systeme mit mindestens 2 Schlössern) ist via optionaler Software eingestellt. Für die Benutzer sind in der Benutzermatrix Freigabe, Öffnen, PIN-Code und / oder Chipkarte (und Unscharf) aktiviert. Der Schlossmaster hat PIN-Code / Codekarten am Schloss angemeldet.



1. Öffnen Sie Schloss 1 gemäß Ihrer Autorisierung.  
*Siehe die Anleitungen zum Öffnen am Anfang des Kapitels. Schloss 1 öffnet sich. Das Display zeigt Öffnen | Schloss auf: 1.*  
Ein anderer, zweiter Benutzer wiederholt Schritt 1 an Schloss 2 und gegebenenfalls tut dies ein dritter an Schloss 3.



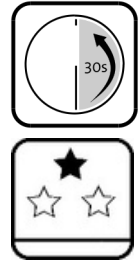
*Das Display zeigt Öffnen | Bitte warten. Der Riegel fährt ein. Das Display zeigt Öffnen | Schloss auf: 2/3.*

Sie haben die Schlösser in Ihrem System erfolgreich geöffnet.

#### 4.12.8 Schloss mit abhängigem Einmalcode öffnen

Siehe auch „Voraussetzungen für abhängigen Einmalcode“ auf Seite 36. Wenn diese Voraussetzungen erfüllt sind, können Benutzer

- mit Personal-/Benutzernummer, mit RFID Karte und Einmalcode oder
  - mit Personal-/Benutzernummer, PIN-Code oder Karte und Einmalcode
- Schlösser öffnen beziehungsweise Personen an Schlössern zulassen.



Vorbedingungen siehe „Voraussetzungen für abhängigen Einmalcode“ auf Seite 36.

1. Drücken Sie kurz die Taste `Clear`, warten Sie etwas und drücken Sie Taste `>`, bis `Oeffnen` angezeigt wird, und Taste `Enter`.  
Das Display zeigt `Code-Eingabe | Schloss1`.
2. Wählen Sie mit `>` und `Enter` gegebenenfalls das Schloss.  
Das Display zeigt `Code-Eingabe | Master` oder `Pers-Nr.`
3. Wählen Sie mit `und` `Enter` oder mit den Zifferntasten und `Enter` Ihre Benutzer- / Personalnummer.  
Das Display zeigt `Benutzer / Pers-Nr` und `Code: .`
4. Geben Sie Ihren PIN-Code ein.  
Das Display zeigt `WTU-Funktion | Code: .`
5. Geben Sie Ihren abhängigen Einmalcode ein.  
*Der Riegel des Schlosses fährt gegebenenfalls ein. Bei Benutzern mit Authentifizierung nur mit PIN-Code zeigt das Display Hallo1, Hallo2 und Hallo3*  
Das Display zeigt `Oeffnen | Bitte warten und Oeffnen | Schloss auf: Nr.` und gegebenenfalls System entsperrt.  
*Falls es sich um einen für Sie als temporären Master generierten Code handelt, können Sie nicht öffnen, sondern eine Person am Schloss zulassen.*

Sie haben das Schloss mit PIN-Code oder Code-Karte oder RFID Karte und abhängigem Einmalcode erfolgreich geöffnet.

#### 4.12.9 Einbruchmeldeanlage (EMA) unscharf schalten

Wenn ein Benutzer nicht zum Unscharf Schalten autorisiert ist, kann er bei angeschlossener und scharf geschalteter EMA kein Schloss öffnen. Das Unscharf Schalten erfolgt automatisch mit dem Öffnen.

Vorbedingungen Für Sie sind PIN-Code und / mindestens Chipkarte, Freigabe, Öffnen und Unscharf aktiviert. TwinAlarm und EMA sind angeschlossen, alle Schlösser geschlossen, TwinAlarm ist aktiviert und die EMA scharf. Der Schlossmaster hat Ihren PIN-Code und Ihre Codekarte am Schloss angemeldet.

gegebenenfalls Chipkarte TwinCard code access.  
Sie benötigen



- Geben Sie Ihren PIN-Code ein und stecken Sie die Codekarte ein.  
*Das Unscharf Schalten erfolgt automatisch beim Öffnen. Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.*

Sie haben geöffnet und die EMA erfolgreich unscharf geschaltet.

#### 4.12.10 Schloss schließen

Wenn ein Schloss schließt, nachdem es via Einmalcode (OTC) geöffnet wurde, wird auf der Bedieneinheit ein 4-stelliger Rückcode WTU-Code: XXXX angezeigt. Dieser Code kann beispielsweise telefonisch weitergegeben und von der Person benutzt werden, die für das Beenden des Vorgangs zuständig ist. Der zuletzt ausgegebene Rückcode kann gegebenenfalls via Menü Status / Info angezeigt werden.



**Vorbedingung** Der Riegelwerkskontakt ist nicht so eingerichtet, dass er bei geschlossenem Riegelwerk ein Schließen des Schlosses verhindert. Über Software ist nicht eingestellt, dass nur mit Code-Eingabe geschlossen werden kann.

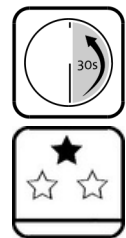
1. Öffnen Sie das Schloss (siehe oben).
2. Wählen Sie mit  $\rightarrow$  und  $\rightarrow$  **Schliessen**.
3. Wählen Sie mit  $\rightarrow$  und gegebenenfalls das Schloss und  $\rightarrow$ .  
*Das Display zeigt Schliessen | Schloss zu: Nr.*

Sie haben das Schloss erfolgreich geschlossen.

#### 4.12.11 Schloss mit Code-Eingabe schließen

Für das Schließen mit Code-Eingabe reicht es aus, entweder PIN- oder Kartencode (TwinCard code access) einzugeben.

**Vorbedingungen** In der PC-Software ist auf Seite „Einstellungen“ Option „Manuelles Schliessen mit Code-Eingabe“ aktiviert. Für Sie sind in der Benutzermatrix Freigabe und Schließen, PIN-Code oder / und Chipkarte aktiviert.



1. Drücken Sie kurz die Taste  $\rightarrow$ .  
*Der Systemstatus wird geprüft. Das Display zeigt Uhrzeit und Datum.*
2. Wählen Sie mit der Taste  $\rightarrow$  **Schliessen** und  $\rightarrow$ .  
*Das Display zeigt Schliessen und gegebenenfalls Schloss 1.*
3. Wählen Sie mit  $\rightarrow$  gegebenenfalls das Schloss und  $\rightarrow$ .  
*Das Display zeigt Code-Eingabe | Benutzer: Master.*
4. Identifizieren Sie sich als Benutzer.  
*Siehe auch „Benutzer- / Personalnummern“ auf Seite 38.*  
*Das Display zeigt gegebenenfalls Benutzer Nr. | PIN-Code.*
5. Wählen Sie **PIN-Code** oder **Codekarte** und schließen Sie das Schloss, indem Sie PIN- / Kartencode eingeben.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels. Das Display zeigt Schliessen | Bitte warten.*  
*Der Schlossriegel fährt aus.*  
*Das Display zeigt Schliessen | Schloss zu: Nr.*

Sie haben das Schloss erfolgreich geschlossen.

#### 4.12.12 Mit Türschalter automatisch schließen

Diese Funktion kann mit PC-Software eingestellt werden.

Vorbedingungen TwinXT (II) / TwinXT small oder TwinAlarm sind angeschlossen und aktiviert. In der PC-Software ist auf Seite „Einstellungen“ Option „Automatisches Schließen mit Türschalter“ aktiviert. Der Riegelwerkskontakt ist nicht so eingerichtet, dass er automatisches Schließen verhindert.

- Schließen Sie die Tür des Wertbehältnisses.  
*Über Tür- und Riegelwerksschalter, deren Zustand regelmäßig geprüft wird, registriert das System das Schließen der Tür des Behältnisses und schließt das Schloss / die Schlösser automatisch, nachdem gegebenenfalls andere Prozesse noch abgeschlossen worden sind.*

Das Schloss hat sich automatisch geschlossen.

#### 4.12.13 Automatisches Schließen TK

Diese Funktion (TK=Türkontakt) kann mit PC-Software eingestellt werden.

Vorbedingungen TwinXT (II) / TwinXT small oder TwinAlarm sind angeschlossen und aktiviert. In der PC-Software ist auf Seite „Einstellungen“ Option „Automatisches Schließen TK [C:1]“ aktiviert. Der Riegelwerkskontakt ist nicht so eingerichtet, dass er automatisches Schließen verhindert.

- Schließen Sie die Tür des Wertbehältnisses.  
*Über Tür- und Riegelwerksschalter, deren Zustand regelmäßig geprüft wird, registriert das System das Schließen der Tür des Behältnisses und schließt das Schloss / die Schlösser sofort automatisch. Andere Prozesse werden gegebenenfalls abgebrochen.*

Das Schloss hat sich automatisch geschlossen.

## Einbruchmeldeanlage (EMA) scharf schalten

Abhängig von der Einstellung in TwinComm („Einstellungen / TwinAlarm / Scharfschalten mit Code“ ein / aus) müssen Benutzer zum Scharf-Schalten PIN-Code eingeben oder Chipkarte einlegen oder nichts von beidem tun. Meist muss die (zuvor angelernte!) Chipkarte eingelegt werden.

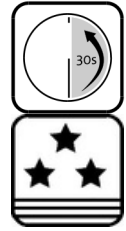
Vorbedingungen TwinAlarm und EMA sind angeschlossen. TwinAlarm ist

aktiviert, EMA unscharf und alle Schlösser sind geschlossen. Nur dann wird Scharfschalten zum

Scharfschalten der EMA

Im versteckten Menü, Untermenü Alarmgeräte hat der Systemmanager TwinAlarm auf aktiv gestellt. Siehe „Verstecktes Menü anzeigen“ auf Seite 60.

Für Sie hat der Systemmanager in der Benutzermatrix Freigabe, PIN-Code und / oder Chipkarte aktiviert.



1. Sperren Sie das System, indem Sie Schloss 1 oder alle Schlösser schließen.  
*Siehe „Systemstatus“ in diesem Kapitel. Das System ist gesichert.*
  2. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
  3. Wählen Sie mit `>` `Scharfschalten` und danach `Enter`.  
*Falls ! EMA scharf ! angezeigt wird, haben Sie die Aufgabe erfolgreich ausgeführt. Springen Sie zum Ende dieser Beschreibung.*  
*Bei aktivierter Option „Scharfschalten mit Code“ zeigt das Display Code-Eingabe | Benutzer: Master und PIN-Code.*
- Identifizieren Sie sich am Schloss und wählen Sie `PIN-Code` / `Codekarte` und `Enter`.  
*Siehe auch „Benutzer- / Personalnummern“ auf Seite 38. Je nach Ihrer Wahl geht es unterschiedlich weiter. Die Code-Eingabe entspricht der beim Öffnen. Siehe die Anleitungen zum Öffnen in diesem Kapitel.*  
*Das Display zeigt Benutzer: Nr. | Bitte warten.*  
*Die Bedieneinheit gibt ein akustisches Signal aus.*  
*Das Display zeigt Benutzer: Nr. | ! EMA Scharf !.*

Sie haben die Einbruchmeldeanlage erfolgreich scharf geschaltet.

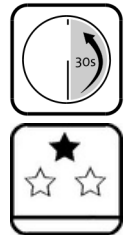
## 4.13 System einrichten

### Vorsicht

Sind in einem Schloss zu wenig öfFnungsberechtigte Benutzer gespeichert, können Sie es nicht öfFnen. Melden Sie in jedem Schloss ausreichend öfFnungsberechtigte Benutzer an, gegebenenfalls auch von jeder an der ÖfFnung beteiligten Gruppe (4-Augen-Prinzip / Parallelcode).

### 4.13.1 Verstecktes Menü anzeigen

Bestimmte grundlegende Einstellungen können über das versteckte Menü gemacht oder überprüft werden. Jeder Benutzer kann das Menü anzeigen. Für bestimmte Einstellungen wie Sprach-Import, Setzen der Zeit und der Einstellung der Alarmgeräte ist der Systemmanagercode, für das Anmelden neuer Benutzer über dieses Menü ist gegebenenfalls Einmalcode (OTC) erforderlich.



1. Drücken Sie eine beliebige Taste und nach 3 Sek. kurz *Clear*.  
Das Display zeigt beispielsweise *Mo 25.09.23 15:50*.
2. Drücken Sie *Enter* und halten Sie die Taste gedrückt.  
*Sprache* wird angezeigt.
3. Bestätigen Sie *Sprache* mit Enter oder wählen Sie mit Taste > einen anderen Menüpunkt und bestätigen Sie diesen mit Enter.  
Die Sprachauswahl, die Einstellungen „Beleuchtung“, „Lautsprecher“ und die Anzeige „Batteriespannung“ erfordern gegebenenfalls keinen Systemmanagercode.  
Um andere Einstellungen vorzunehmen, geben Sie den Systemmanagercode ein und nehmen Sie anschließend die Einstellung vor.
- 4.

Sie haben erfolgreich das versteckte Menü angezeigt.

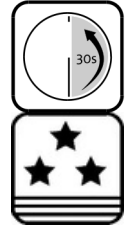
## 4.13.2 Einstellungen: Schlosssystem

Über dieses Menü, das gegebenenfalls ab den Softwareversionen LP/LQ11 und ab LP21 verfügbar ist, können Sie die folgenden Parameter auch ohne andere Software konfigurieren.

### 4.13.2.1 Codeverknüpfung

Möglichkeit der Einstellung von Codeverknüpfung / 4-Augen-Prinzip für das Öffnen, für die Konfiguration und für die Freigabezeit.

Bei Einstellung der jeweiligen Option können nur noch 2 Benutzer gemeinsam Schlösser öffnen oder Parameter ändern oder, wenn „Freigabezeit“ eingestellt ist, müssen 2 Benutzer nach der Öffnung während der Freigabezeit Code eingeben.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit `>Einstellungen` und `Enter`.  
*Das Display zeigt `Einstellungen | Mastercodes`.*
3. Wählen Sie mit `> Schlosssystem` und danach `Enter`.  
*Das Display zeigt `Code-Eingabe Systemmanager, gegebenenfalls 0123456789` und `Code: . Siehe auch Abschnitt „PIN-Code eingeben“`.*
4. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt `Oeffnen`.*
5. Wählen Sie mit `Enter Oeffnen` oder mit `> und Enter Konfiguration` oder `Freigabezeit`.  
*\*=JA | \*=Nein wird angezeigt.*
6. Wählen Sie die gewünschte Option mit `<` oder `>` und `Enter`.  
*Das Programm nimmt die gewünschte Einstellung vor.*

Sie haben erfolgreich Codeverknüpfung für die von Ihnen gewählte Funktion eingestellt.

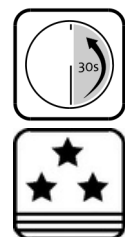
### 4.13.2.2 Parallelcode

Möglichkeit der Einstellung von Parallelcode für ein Schlosssystem mit (mindestens) 2 Schlössern.

Der erste Benutzer kann Schloss 1, 2 oder 3 öffnen, der zweite das andere oder eines der beiden noch geschlossenen und der dritte gegebenenfalls das letzte.

Kombinierbar mit „Zwangsfolge“. Wenn 2 Schlösser im System sind, kann ein Benutzer während einer „Teilsperrezeit“ ein Wertbehältnis auch alleine öffnen.

Bei Aktivierung dieser Funktion mit der optionalen PC-Software wird die Funktion „Codeverknüpfung“ automatisch deaktiviert. Aktivierung ähnlich „Codeverknüpfung“ (siehe oben).



#### 4.13.2.3 Zwangsfolge

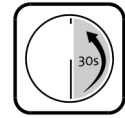
Möglichkeit der Einstellung von Zwangsfolge für ein Schlosssystem mit (mindestens) 2 Schlössern.

Möglichkeit, eine Reihenfolge festzulegen, die beim Öffnen und Schließen der Schlösser eingehalten werden muss.

Wenn Sie die Option „Zwangsfolge“ wählen, müssen Benutzer zuerst Schloss 1, dann Schloss 2 und danach gegebenenfalls Schloss 3 öffnen. Die Abfolge wird durch das Schlosssystem vorgegeben. Der Bediener hat darauf keinen Einfluss. Diese Funktion vereinfacht die Bedienung. Nach der Öffnung von Schloss 1 ist das System teilgesichert (entspricht bei Option ZF dem Zustand „gesichert“), nach der Öffnung aller Schlösser ist das System entsperrt und damit ungesichert.

Beim Schließen muss zuerst gegebenenfalls Schloss 3, dann Schloss 2 und zuletzt Schloss 1 geschlossen werden. Danach ist das System gesichert.

Werkseinstellung: deaktiviert. Aktivierung ähnlich Codeverknüpfung (siehe oben).



#### 4.13.2.4 Zeitverzögerung

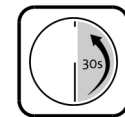
Möglichkeit der Einstellung verschiedener Arten von Zeitverzögerung für Schlösser oder für Personen, denen Wochenprogramme zugeordnet sind. Einzustellen sind jeweils 3 zweistellige Werte in Minuten

00<00<00.

Der erste Wert entspricht jeweils der Öffnungsverzögerung, der zweite der Freigabezeit und der dritte der Alarmverzögerung oder der Öffnungs-

verzögerung nach stillem Alarm.

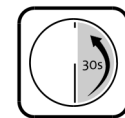
Werkseinstellung: deaktiviert. Aktivierung ähnlich Codeverknüpfung (siehe oben).



#### 4.13.2.5 Wochenprogramme

Möglichkeit der Erstellung von 5 Wochenprogrammen. Einzustellen sind jeweils für jeden Wochentag jeweils 2 Uhrzeiten, der Anfangs- und der Ende-Zeitpunkt, beispielsweise Mo:07:00-12:00.

Im festgelegten Zeitraum kann jeweils geöffnet werden. Werkseinstellung: deaktiviert. Die erstellten Wochenprogramme können bei der Neuanlage von Benutzern diesen Benutzern zugeordnet werden. Aktivierung ähnlich Codeverknüpfung (siehe oben).



### 4.13.3 Datum und Uhrzeit einstellen

Von der richtigen Einstellung von Datum und Uhrzeit sind alle Zeitfunktionen des Systems abhängig, ebenso das Ereignisprotokoll. Die Sommer- / Winterzeit-Umstellung erfolgt werkseingestellt automatisch.



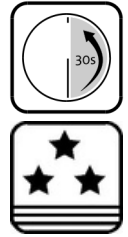
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Das Display zeigt **Oeffnen oder Schliessen**.*
2. Wählen Sie mit Taste > **Einstellungen** und Enter.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit Taste > **Datum/Uhrzeit** und Enter.  
*Das Display zeigt **Systemmanager | Code-Eingabe** und **Code:..***
4. Geben Sie den Systemcode ein.  
*Uhrzeit und Datum werden angezeigt. Im Display blinkt die erste Ziffer der Uhrzeit. Wenn Sie die Zeiteinstellung behalten wollen, drücken Sie 2x **Clear**.*
5. Geben Sie die erste Ziffer der aktuellen Uhrzeit ein und wählen Sie **Enter**.  
*Fahren Sie mit der Eingabe fort, bis der aktuelle eingestellte Wochentag blinkt.*
6. Wählen Sie mit > den aktuellen Wochentag und Enter.  
*Der Cursor blinkt auf der ersten Ziffer des Datums.*
7. Geben Sie Tag, Monat und Jahr ein.  
*Das Display zeigt **Manager | Code ändern**.*

Sie haben Datum und Uhrzeit erfolgreich eingestellt.

## 4.13.4 Alarmgeräte einstellen / ein- / ausschalten

## Vorsicht

Gefahr, dass nach dem Aktivieren der Erweiterungseinheit bei Öffnungsversuch am Schloss „Keine Freigabe“ angezeigt wird.  
 Nach dem Aktivieren der Erweiterungseinheit werden beide Eingänge in Funktion gesetzt.  
 Deaktivieren Sie Eingang „Freigabe“ via optionale PC-Software, wenn möglich.



Vorbedingungen Alarmgerät im System verfügbar.

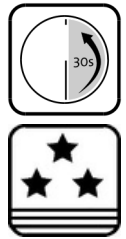
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Das Display zeigt* `OeffnenoderSchliessen`.
2. Wählen Sie mit den Tasten `>` und `Enter` `Einstellungen`.  
*Das Display zeigt* `Einstellungen | Mastercode`.
3. Wählen Sie mit `>` und `Enter` `Alarmgeräte`.  
*Das Display zeigt* `Systemmanager | Code:.`
4. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt* `Alarmgeraete | XT-Erweiterung`.
5. Wählen Sie mit `>` und `Enter` `XT-Erweiterung` oder `TwinAlarm`.  
*Das Display zeigt zum Beispiel* `XT-Erweiterung | * = JA * = NEIN`.
6. Wählen Sie mit `>` und `Enter` `* = JA`, oder `* = NEIN`.  
*Falls TwinXT mit \* = NEIN deaktiviert wurde,*  
*zeigt das Display* `XT-Erweiterung aktiv | Geloescht`.  
*Im anderen Fall zeigt das Display beispielsweise* `A:1<B:1R:1F:0C:0`.  
*A = Auswertung der Eingänge Riegelwerk /Freigabe (0=offen/1=geschlossen)*  
*B = boltwork / Riegelwerk (0=nicht aktiv/1=aktiv)*  
*R = Release / Freigabe (0=nicht freigegeben, 1= freigegeben)*  
*F = Umleitung Riegelwerk an Tastatur (nur bei A=1 möglich)*  
*C = Automatisches Schließen mit TK (Türkontakt)*  
*< = Stellung des Cursors*  
*0 = nicht aktiv; 1 = aktiv.*  
*Im Fall von C bedeutet 0 = NO, normal open; 1 = NC, normal closed.*
7. Wählen Sie mit `1` oder `0` und `Enter` die gewünschten Einstellungen.  
*Das Display zeigt beispielsweise* `XT-Erweiterung aktiv | Gespeichert`.

Sie haben erfolgreich ein Alarmgerät eingestellt und / oder ein- oder ausgeschaltet.

#### 4.13.5 WTU-Funktion / Zwei ‚Benutzergruppen‘ wählen / Zähler-Reset

Siehe auch ‚Bedienung mit ‚Benutzergruppen‘ aktiviert‘ auf Seite 39.

Verwenden Sie diese Vorgehensweise auch, um den Vorgangszähler des Schlosses auf null zurückzusetzen, wenn gewünscht. Zu diesem Zweck reicht es, die aktuelle Einstellung (WTU JA/NEIN) zu bestätigen



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit Menütaste > **Einstellungen** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Einstellungen | Mastercodes**.*
3. Wählen Sie mit > **WTU-Funktion** und wieder **Enter**.  
*Das Display zeigt **Code-Eingabe, Systemmanager und Code:**.*
4. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt **WTU-Funktion/\*=JA \*=NEIN**. Um den Vorgangszähler auf 0 zu setzen, bestätigen Sie die aktuelle Einstellung.*
5. Wählen Sie mit > zum Aktivieren **\*=JA**, zum Deaktivieren **\*=NEIN** und erneut **Enter**.  
*Das Display zeigt **WTU-Funktion | Geloescht** oder **WTU-Funktion | Gespeichert**.*

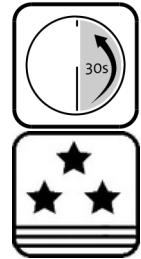
Sie haben die WTU-Funktion erfolgreich ein- oder ausgeschaltet / den Vorgangszähler erfolgreich auf „0“ gesetzt.

## 4.14 Verwaltung und Benutzer

### 4.14.1 Systemmanagercode ändern

Der Systemmanagercode des Schlosses (=Systemcode) berechtigt nicht zur Schlossöffnung, sondern zur Systemkonfiguration.

**Vorsicht**



Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert.

Ändern Sie werksseitigen Code so bald wie möglich.

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden. Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

Ohne Systemmanagercode können Sie Ihr System nicht mehr konfigurieren.

Speichern Sie den Systemmanagercode an einem sicheren, nur dem Systemmanager zugänglichen Ort.

Gefahr von Funktionsausfall.

Stellen Sie sicher, dass der Systemmanagercode in allen Schlössern des Systems jeweils gleich lautet. Nutzen Sie die Kopierfunktion.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit Taste > **Einstellungen** und Taste Enter.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit Taste > **Managercode** und Enter.  
*Das Display zeigt **Code-Eingabe | Schloss 1**.*
4. Bei 2 oder 3 Schlössern im System wählen Sie Schloss 1 mit **Enter**.  
*Das Display zeigt **Code-EingabeSystemmanager ... und Code:**.*
5. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt **Systemmanager | Bitte warten**,  
danach **Managercode neu | Code:**.*
6. Geben Sie den neuen Systemmanagercode ein.  
*Das Display zeigt **Code bestätigen | Code:**.*
7. Wiederholen Sie die Eingabe des neuen Systemmanagercodes.  
*Das Display zeigt **Managercode neu | Bitte warten**  
und danach **Managercode neu | Gespeichert**.*

Sie haben den Systemmanagercode erfolgreich geändert.

#### 4.14.2 Mastercode / WTU-Mastercode ändern

Der Master- und gegebenenfalls der WTU-Mastercode eines Schlosses berechtigen zum Verwalten der Benutzer des Schlosses sowie optional auch zum Öffnen des Schlosses.



#### Vorsicht

Mit werksseitigem Mastercode ist das System nicht gesichert.  
Ändern Sie werksseitigen Code so bald wie möglich.

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.  
Gefahr der unberechtigten Öffnung.  
Wählen Sie keine derartigen Codes.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

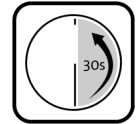
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ auf Seite 37.*
2. Wählen Sie mit Taste > `Einstellungen` und Taste `Enter`.  
*Das Display zeigt `Einstellungen | Mastercode`.*
3. Bestätigen Sie `Mastercode` mit `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
4. Wählen Sie mit < und > gegebenenfalls das Schloss, dessen Mastercode Sie ändern möchten, und wieder `Enter`.  
*Das Display zeigt `Mastercode | Code-Eingabe und Code:`.*  
  
*Bei WTU-Betrieb zeigt das Display `Code-Eingabe und Benutzer: Master`. Sie können mit < und > WTU-Master wählen. In allen anderen Punkten entspricht diese Codeänderung derjenigen des Mastercodes.*
5. Geben Sie den Master- beziehungsweise den WTU-Mastercode ein.  
*Das Display zeigt `Mastercode | Bitte warten`, dann `Mastercode neu, gegebenenfalls 0123456789` und `Code:`.*
6. Geben Sie den neuen (WTU-)Mastercode ein.  
*Das Display zeigt `Code bestätigen und Code:`.*
7. Wiederholen Sie Ihre Eingabe des neuen (WTU-)Mastercodes.  
*Das Display zeigt `Mastercode neu | Bitte warten`, und `Mastercode neu | Gespeichert`.*

Sie haben den Master- oder den WTU-Mastercode erfolgreich geändert.

## PIN-Code für Benutzer anmelden

Der Schlossmaster und gegebenenfalls auch der WTU-Master können PIN-Codes für Benutzer am Schloss anmelden.

Damit ein Benutzer ein Schloss mit PIN-Code öffnen kann, muss er dafür in der Benutzermatrix der PC-Software autorisiert worden sein.



### Vorsicht

Wenn bei Systemen mit TwinAlarm die PIN-Codes vor der Installation und der Aktivierung von TwinAlarm angemeldet werden, werden die PIN-Codes der Benutzer nicht in TwinAlarm gespeichert.

Stellen Sie sicher, dass TwinAlarm installiert und aktiviert ist (siehe "Alarmgeräte einstellen / ein- / ausschalten" auf Seite 64), bevor Sie PIN-Codes am Schloss anmelden.

Vorbedingungen Wenn eine Einbruchmeldeanlage Teil des Systems ist, muss TwinAlarm installiert und aktiviert sein.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ auf Seite 37.*
2. Wählen Sie mit Taste `> Einstellungen` und `Enter`.  
*Das Display zeigt `Einstellungen | Mastercode`.*
3. Wählen Sie mit `> PIN-Code` und danach `Enter`.  
*Das Display zeigt `PIN-Code | Anmelden`.*
4. Bestätigen Sie `Anmelden` mit `Enter`.  
*Das Display zeigt `Anmelden | Code aendern`.*
5. Wählen Sie mit `> Benutzer neu` und danach `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
6. Wählen Sie mit `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt bei WTU-Betrieb:  
`Code-Eingabe | Benutzer: Master`.  
Mit `<` und `>` können Sie WTU-Master wählen und `Enter` drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master ...`  
und `Code:`.*
7. Geben Sie den Mastercode (den WTU-Mastercode) ein.  
*Das Display zeigt `(WTU-)Mastercode | Bitte warten`  
und danach `Anmelden | Benutzer: 01`.*
8. Wählen Sie mit den Ziffern- oder den Menütasten `<` und `>` und `Enter` den Benutzer, für den Sie Code anmelden möchten.  
*Das Display zeigt `Benutzercode neu | Code:`.*
9. Geben Sie den neuen Benutzercode ein.  
*Das Display zeigt `Code bestaetigen | Code:`.*

10. Wiederholen Sie die Eingabe des neuen Benutzercodes.

*Das Display zeigt PIN-Code | Bittewarten und danach Benutzer Nr. | Gespeichert. Danach zeigt das Display ab Version LP11 Wochenprogramm 1 | \*=JA | \*=Nein.*

11. Wählen Sie gegebenenfalls mit Taste < oder > und / oder **Enter**, ob dem Benutzer Wochenprogramm 1 zugeordnet werden soll.

*Das Display zeigt Wochenprogramm 2 | \*=JA | \*=Nein.*

12. Wählen Sie gegebenenfalls ebenso, ob dem Benutzer die Wochenprogramme 2-5 zugeordnet werden sollen.

*Code kopieren? | \*=JA | \*=Nein zeigt das Display, wenn 2 Schlösser im System sind.*

13. Wählen Sie gegebenenfalls mit Taste < oder > und / oder **Enter**, dass der Benutzercode auf das andere Schloss kopiert werden soll.

*Die Zuordnung zu den Wochenprogrammen wird gegebenenfalls auch kopiert. Das Display zeigt PIN-Code | Bitte warten und danach Benutzer Nr. | Gespeichert. Das Display zeigt Weiterer Code? | \*=JA | \*=Nein.*

14. Wählen Sie **\*=JA**, wenn Sie weitere PIN-Codes anmelden wollen.

Für jede weitere Anmeldung wiederholen Sie die Schritte 8 bis 13.

Wählen Sie **\*=Nein**, wenn Sie das Anmelden beenden wollen.

Sie haben erfolgreich PIN-Code für Benutzer angemeldet.

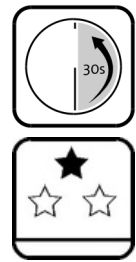
#### 4.14.4 PIN-Code ändern

Jeder Benutzer kann bei seinem System seinen PIN-Code ändern.

##### Vorsicht

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden. Gefahr der unberechtigten Öffnung. Wählen Sie keine derartigen Codes.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.



**Vorbedingungen** Für Sie sind in der Benutzermatrix (PC-Software) mindestens PIN-Code und Freigabe aktiviert. Der Schlossmaster hat Ihren PIN-Code am Schloss angemeldet.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie **Einstellungen** mit Taste **>** und **Enter**.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit **>PIN-Code** und danach **Enter**.  
*Das Display zeigt **PIN-Code | Anmelden**.*
4. Bestätigen Sie **Anmelden** mit **Enter**.  
*Das Display zeigt **Anmelden | Code ändern**.*
5. Bestätigen Sie **Code ändern** mit **Enter**.  
*Das Display zeigt gegebenenfalls **Alter Code | Schloss 1**.*
6. Wählen Sie mit **<** und **>** gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt **Alter Code | Benutzer: 01**.*
7. Identifizieren Sie sich als Benutzer.  
*Siehe auch „Benutzer- / Personalnummern“ auf Seite 38.  
Das Display zeigt **Benutzer: ... und Code:**.*
8. Geben Sie Ihren bisherigen Code ein.  
*Das Display zeigt **Benutzercode neu ... und Code:**.*  
*Siehe auch „PIN-Code eingeben“ auf Seite 47.*
9. Geben Sie Ihren neuen Code ein.  
*Das Display zeigt **Code bestätigen ... und Code:**.*
10. Geben Sie Ihren neuen Code nochmals ein.  
*Das Display zeigt **PIN-Code | Bitte warten**.  
Das Display zeigt **PIN-Benutzer: | Gespeichert**.*

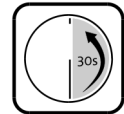
Sie haben erfolgreich Ihren PIN-Code geändert.

#### 4.14.5 PIN-Code abmelden

Der Schlossmaster und gegebenenfalls auch der WTU-Master können PIN-Codes für Benutzer am Schloss abmelden.

##### Vorsicht

Gefahr eines Konfigurationsfehlers: Wertbehälter kann möglicherweise nicht mehr geöffnet werden. Wenn Sie „Codeverknüpfung“ oder „Zwangsfolge“ eingerichtet haben, melden Sie an jedem Schloss mindestens so viele zur Öffnung autorisierte Codes an wie benötigt. Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden.



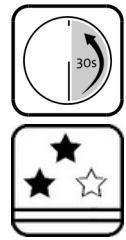
1. Wählen Sie Menü `Einstellungen | PIN-Code`.  
*Eine genaue Anleitung hierfür siehe obige Beschreibung „PIN-Code ändern“, Schritte 1-3 auf Seite 70. Das Display zeigt PIN-Code | Anmelden.*
2. Wählen Sie mit `>` `Abmelden` und Taste `Enter`.  
*Das Display zeigt gegebenenfalls `Code-Eingabe | Schloss 1`.*
3. Wählen Sie gegebenenfalls mit `>` das Schloss und `Enter`.  
*Das Display zeigt bei WTU-Betrieb:  
`Code-Eingabe | Benutzer: Master`.  
Mit `>` können Sie WTU-Master wählen und `Enter` drücken.  
  
Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master..` und `Code:`.*
4. Geben Sie den (WTU-)Mastercode ein.  
*Das Display zeigt `(WTU-)Mastercode | Bitte warten` und danach `Abmelden | Benutzer: XX`.*
5. Wählen Sie mit den Ziffern- oder den Menütasten `<` und `>` den Benutzer, dessen Code Sie abmelden möchten, und `Enter`.  
*Das Display zeigt `PIN-Code | Bitte warten` und `Benutzer XX | Geloescht`.  
`Schloss 2` und `Code loeschen? | *=JA | *=Nein` zeigt das Display, wenn 2 Schlösser im System sind.*
6. Wählen Sie `*=JA`, wenn Sie ihn auch an Schloss 2 abmelden wollen.  
*Danach zeigt das Display `Weiterer Code? | *=JA | *=Nein`.*
7. Wählen Sie `*=JA`, wenn Sie weitere PIN-Codes abmelden wollen.  
Für jede weitere Abmeldung wiederholen Sie Schritt 5 (und optional 6).  
Wählen Sie `*=Nein`, wenn Sie das Abmelden beenden wollen.

Sie haben erfolgreich PIN-Code abgemeldet.

#### 4.14.6 PIN-Code Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls auch der WTU-Master können anzeigen lassen, welche Benutzercodes angemeldet sind. Beide können nur die Benutzer ihres Benutzerbereichs sehen.

Auch nach Umstellung auf Personalnummern (möglich ab Version LP09) werden in den Menüs „Benutzer-Anzeige“ und „PIN-Code abmelden“ auf dem Display Benutzernummern angezeigt.



1. Wählen Sie Menü **Einstellungen | PIN-Code**.  
*Eine genaue Anleitung hierfür siehe obige Beschreibung „PIN-Code ändern“, Schritte 1-3 auf Seite 70. Das Display zeigt PIN-Code | Anmelden.*
2. Wählen Sie mit **>** **Benutzer-Anzeige** und Taste **Enter**.  
*Das Display zeigt gegebenenfalls Code-Eingabe | Schloss 1.*
3. Wählen Sie gegebenenfalls mit **>** das Schloss, dem Sie als Master zugeordnet sind, und bestätigen Sie mit **Enter**.  
*Das Display zeigt bei WTU-Betrieb:  
Code-Eingabe | Benutzer: Master.  
Mit **<** und **>** können Sie WTU-Master wählen und **Enter** drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master ... und Code:.*
4. Geben Sie den Mastercode (den WTU-Mastercode) ein.  
*Das Display zeigt Master | Bitte warten und danach:  
PIN-Benutzer: XXX | Ben-Code Nr.: OK/NOK.  
Oben wird die Anzahl der angemeldeten PIN-Codes angezeigt, unten jeweils eine Benutzernummer und OK oder NOK.*
5. Blättern Sie mit **<** und **>** durch die Nummern der Benutzer.  
*OK oder NOK zeigen, ob PIN-Code angemeldet ist:  
NOK bedeutet, dass für den Benutzer kein PIN-Code angemeldet ist.  
OK bedeutet, dass für den Benutzer PIN-Code angemeldet ist.*

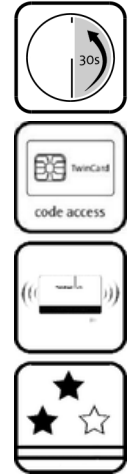
Sie haben erfolgreich angezeigt, für wie viele und für welche Benutzer PIN-Code angemeldet ist.

#### 4.14.7 Codekarte anmelden (auch RFID-Karten)

Der Schlossmaster und gegebenenfalls auch der WTU-Master können Codekarten anmelden. Vorher gegebenenfalls TwinAlarm aktivieren. Damit ein Benutzer Schlösser mit Karte öffnen kann, muss er dazu autorisiert sein (u.a. Berechtigung „Karte“ in Benutzermatrix).

Sie benötigen eine TwinCard code access / RFID-Karte pro Benutzer.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Taste > **Einstellungen** und **Enter**.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit > **Codekarte** und danach **Enter**.  
*Das Display zeigt **Codekarte | Anmelden**.*
4. Bestätigen Sie mit **Enter**.  
*Das Display zeigt **Code-Eingabe | Schloss 1**.*
5. Wählen Sie mit > gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt bei WTU-Betrieb: **Code-Eingabe | Benutzer: Master**. Mit < und > können Sie WTU-Master wählen und **Enter** drücken. Ohne aktivierte WTU-Funktion zeigt das Display **Code-Eingabe, Master und Code:**.*
6. Geben Sie den (WTU-)Mastercode ein.  
*Das Display zeigt **Anmelden | Benutzer: (WTU-)Master**.*
7. Wählen Sie die Nummer des Benutzers, für den Sie die Codekarte anmelden, mit den Zifferntasten oder mit < und > und **Enter**.  
*Das Display zeigt **Benutzer: Nr. | Karte ein**.  
Das Display zeigt bei RFID-Karten **Benutzer: Nr. | Lese Daten**.*
8. Stecken Sie die Chipkarte in den Kartenleser von FlatControl beziehungsweise halten Sie die RFID-Karte vor FlatControl / die Optionsbox von QPad.  
*Siehe die Anleitung auf Seite 49 und 50.  
Das Display zeigt **Bitte warten und bei Chipkarten Karte aus**.*
9. Entfernen Sie die Karte.  
*Das Display zeigt **Benutzer Nr. | Angemeldet**. Danach zeigt das Display ab Version LP11 **Wochenprogramm 1 | \*=JA | \*=Nein**.*
10. Wählen Sie gegebenenfalls mit Taste < oder > und / oder **Enter**, ob dem Benutzer die Wochenprogramme 1-5 zugeordnet werden soll.  
*Das Display zeigt gegebenenfalls **Wochenprogramm | Gespeichert**. Es zeigt **Code kopieren? | \*=JA | \*=Nein** mit 2 Schlössern im System.*
11. Wählen Sie gegebenenfalls mit Taste < oder > und / oder **Enter**, dass die Codekarte auf das andere Schloss kopiert werden soll.  
*Die Zuordnung zu den Wochenprogrammen wird gegebenenfalls auch kopiert. Danach zeigt das Display **Weiterer Code? | \*=JA | \*=Nein**. Sie können mit \*=JA weitere Codekarten anmelden, indem Sie jeweils die Schritte 7-10 mit neuen Daten wiederholen.*



Sie haben erfolgreich eine neue Codekarte angemeldet.

#### 4.14.8 Codekarte abmelden (auch RFID-Karten)

Der Schlossmaster und gegebenenfalls auch der WTU-Master können angemeldete Codekarten wieder abmelden. Selbst wenn ein Benutzer zum Schloss-Öffnen mit Codekarte autorisiert ist, kann er ein Schloss nicht öffnen, wenn seine Karte abgemeldet ist.



#### Vorsicht

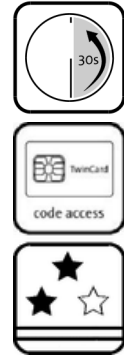
Gefahr eines Konfigurationsfehlers: Schloss kann möglicherweise nicht mehr geöffnet werden. Wenn Sie Option „Codeverknüpfung“ oder „Zwangsfolge“ aktiviert haben, melden Sie an jedem Schloss mindestens so viele zur Öffnung autorisierte Codes an wie benötigt. Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden.

1. Wählen Sie Menü **Einstellungen | Codekarte**.  
*Genauere Anleitung siehe obige Beschreibung „Codekarte anmelden (auch RFID-Karten)“, Schritte 1-3 auf Seite 73.*  
*Das Display zeigt Codekarte | Anmelden.*
2. Wählen Sie mit **> Abmelden** und bestätigen Sie mit **Enter**.  
*Das Display zeigt Code-Eingabe | Schloss 1.*
3. Wählen Sie mit **>** gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt bei WTU-Betrieb: Code-Eingabe | Benutzer: Master.*  
*Mit **>** können Sie WTU-Master wählen und **Enter** drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master.. und Code:.*
4. Geben Sie den (WTU-)Mastercode ein.  
*Das Display zeigt Bitte warten und Abmelden | Benutzer: (WTU-)Master.*
5. Wählen Sie mit **<** und **>** den Benutzer, dessen Codekarte Sie abmelden möchten, und bestätigen Sie mit **Enter**.  
*Das Display zeigt Benutzer Nr. | Bitte warten und Benutzer Nr. | Abgemeldet.*  
*Schloss 2 und Code löschen? | \*=JA | \*=Nein zeigt das Display, wenn 2 Schlösser im System sind.*
6. Wählen Sie **\*=JA**, wenn Sie die Karte auch an Schloss 2 abmelden wollen.  
*Danach zeigt das Display Weiterer Code? | \*=JA | \*=Nein.*
7. Wählen Sie **\*=JA**, wenn Sie weitere Codekarten abmelden wollen.  
Für jede weitere Abmeldung wiederholen Sie die Schritte 5 und 6.  
Wählen Sie **\*=Nein**, wenn Sie das Abmelden beenden wollen.

Sie haben eine Codekarte erfolgreich abgemeldet.

#### 4.14.9 Codekarte Benutzer-Anzeige (auch RFID Karten)

Der Schlossmaster und gegebenenfalls auch der WTU-Master können anzeigen, für welche Benutzer Codekarten am Schloss angemeldet sind. Bei WTU-Betrieb können Master und WTU-Master jeweils nur die Benutzer ihres Benutzerbereichs anzeigen.



1. Wählen Sie Menü **Einstellungen | Codekarte**.  
*Genauere Anleitung siehe obige Beschreibung „Codekarte anmelden“, Schritte 1-3 auf Seite 73.*  
*Das Display zeigt Codekarte | Anmelden.*  
 > Benutzer-Anzeige
2. Wählen Sie mit < und > **Code-Eingabe | Schloss** und **Enter**.  
*Das Display zeigt 1.*
3. Wählen Sie mit < und > gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt bei WTU-Betrieb:*  
*Code-Eingabe | Benutzer: Master.*  
*Mit < und > können Sie WTU-Master wählen und **Enter** drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master ... und Code:.*  
 Geben Sie den (WTU-)Mastercode ein.
4. *Das Display zeigt Bitte warten und*  
*danach Karten 000 | Karte 00 (N)OK.*  
*Oben wird die Anzahl der angemeldeten Codekarten angezeigt,*  
*unten jeweils eine Benutzernummer und OK oder NOK.*
5. Blättern Sie mit < und > durch die Nummern der Benutzer.  
*OK und NOK zeigen, ob Codekarten registriert sind:*  
*NOK bedeutet, dass für den Benutzer keine Karte angemeldet ist.*  
*OK bedeutet, dass für den Benutzer eine Codekarte angemeldet ist.*

Sie haben erfolgreich angezeigt, für welche und für wie viele Benutzer Codekarten angemeldet sind.

## 4.15 Service

### 4.15.1 Status / Info des Systems anzeigen



1. Drücken Sie kurz **Enter**.  
*Das Display zeigt **Oeffnen** oder **Schliessen**.*
2. Wählen Sie mit den Tasten **<** und **>** **Status / Info** und bestätigen Sie mit **Enter**.  
*Es werden angezeigt:*
  - System Check, VdS Klasse System, Zustand der Schlösser (auf / Mitte / zu)
  - Zustand des Systems (entsperrt / teilgesperrt / gesichert)
  - Zustand einer optionalen Einbruchmeldeanlage (scharf / unscharf)
  - Firmware-Version des Terminals / RFID-Moduls (optional)
  - Firmware-Version von Schloss
  - Basic Firmware des Schlosssystems
  - aktueller Rückcode **WTU-Code: XXXX**, falls vorhanden
  - Spannung

Sie haben Informationen zu Systemkomponenten erfolgreich angezeigt.

## 4.15.2 Service Reset

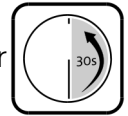
Der Systemmanager kann mit Menü **Reset** die aktuellen Einstellungen und Benutzercodes löschen und die Werkseinstellungen wiederherstellen.

### Vorsicht

Durch das Laden der Werkseinstellungen werden für das System spezifische, auch Hardware- und Benutzer-Einstellungen gelöscht.

Nach dem Hochfahren kann gegebenenfalls nur der jeweilige Schlossmaster öffnen.

Speichern Sie die aktuelle Konfiguration mit optionaler Software, bevor Sie die Werkseinstellungen laden.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Das Display zeigt **Oeffnen** oder **Schliessen**.*
2. Wählen Sie mit Taste **>** **Service** und Taste **✓** **Enter**.  
*Das Display zeigt **Service | Reset**. Falls **Service** nicht verfügbar ist, öffnen Sie das Schloss / die Schlösser.*
3. Bestätigen Sie mit **Enter**.  
*Das Display zeigt **Code-Eingabe** und **Systemmanager**, gegebenenfalls **0123456789** und **Code:.***
4. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt **Systemmanager** und **Terminal**. Sie können wählen, ob Sie mit **Terminal** das ganze System oder mit **Schloss** ein Schloss auf die Werkseinstellungen zurücksetzen wollen.*
5. Bestätigen Sie mit **Enter** oder wählen Sie **Schloss** und **Enter**, sowie gegebenenfalls **Schloss 1**, **Schloss 2** oder **Schloss 3** und **Enter**.  
*Das Display zeigt **Code-Eingabe** und **Systemmanager**, gegebenenfalls **0123456789** und **Code:.***
6. Geben Sie den Systemmanagercode nochmals ein.  
*Angezeigt werden **Systemmanager | Bittewarten** und **INITIALISIERUNG | EEPROM LOESCHEN, OK, TwinLock** und **System Setup**.*
7. Bestätigen Sie mit **Enter**.  
*Das Display zeigt gegebenenfalls **Sprache | 1 Deutsch**. Mit **Enter** können Sie bestätigen, mit **<** oder **>** können Sie eine andere Sprache wählen.*
8. Bestätigen Sie die gewählte Sprache mit **Enter**.  
*Das Display zeigt **Deutsch | Gespeichert** und danach **System - Setup | Neues System**.*
9. Wählen Sie mit **<** oder **>** **Terminal - Wechsel** und **Enter**.  
*Das Display zeigt **System - Setup | Terminal: 1**.*
10. Bestätigen Sie mit **Enter**.  
*Das Display zeigt **System - Setup | Anzahl DMS: 1**.*
11. Wählen Sie mit **<** oder **>** die Anzahl der Schlösser und **Enter**.  
*Das Display zeigt **Seriennummer | Schloss 1** und **Code-Eingabe | Systemmanager** und **Code:.***

12. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt Seriennummer | Bitte warten.*  
*Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.*  
*Das Display zeigt Seriennummer | Gespeichert.*  
*Bei mehreren Schlössern im System zeigt das Display*  
*Seriennummer | Schloss 2 und*  
*Code-Eingabe | Manager und Code:.*  
 Geben Sie gegebenenfalls den Managercode des Schlosses 2 ein.
13.  
*Werkseingestellt entsprechend diese dem Systemmanagercode ab Werk.*  
*Das Display zeigt Seriennummer | Bitte warten.*  
*Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.*  
*Das Display zeigt Seriennummer | Gespeichert.*  
*Nach dem letzten Schloss zeigt das Display Datum/Uhrzeit und*  
*Code-Eingabe | Systemmanager und Code:.*
14. Wählen Sie die Ziffern des Systemmanagercodes.  
*System-Uhrzeit und Datum werden angezeigt.*
15. Drücken Sie die Taste `Enter`, um Uhrzeit und Datum einzustellen.
16. Geben Sie die Uhrzeit mit `<` und `>` und Enter oder mit den Zifferntasten ein.  
*Im Display blinkt der Cursor vor dem eingestellten Wochentag.*
17. Wählen Sie mit `<` und `>` die beiden ersten Buchstaben des aktuellen Wochentags und bestätigen Sie mit Enter.  
*Im Display blinkt der aktuell eingestellte Tag.*
18. Geben Sie Tag, Monat und Jahr ein.  
*Das Display zeigt Datum/Uhrzeit | Gespeichert.*  
*Das Display zeigt Schlosssystem | Angemeldet.*  
*Danach zeigt das Display gegebenenfalls Anzahl DMS Aussentuer: 0*  
*und danach Anzahl DMS Innentuer: 0.*
19. Geben Sie die Anzahl der Schlösser in Innen- / Außentür ein, falls erforderlich.  
*Schlosssystem | Angemeldet*  
 und  
*TwinLock Business | 22.09.23* wird angezeigt.

Sie haben erfolgreich ein Reset durchgeführt.

### 4.15.3 Motor-Service / Motor Schritt

Schlossmaster können mit Menü Motor

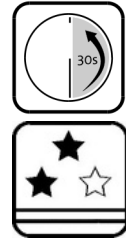
Service den Schlossriegel

schrittweise ein- und ausfahren und so den Mechanismus testen.

#### Hinweis

Falls mit der optionalen PC-Software „automatisches Schließen“ eingestellt wurde, schließt das System das Schloss eine Minute nach der Ausführung der hier beschriebenen Motorschritte.

Falls nicht, bleibt der Riegel in der Position, in die er mit dem letzten Motorschritt gefahren wird.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit der Taste `>` `Service` und Taste `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Wählen Sie mit `>` `Motor-Service` und wieder `Enter`.  
*Das Display zeigt `Service | Motor-Service`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 01`.*
5. Wählen Sie mit `>` gegebenenfalls das Schloss, dessen Riegel Sie schrittweise bewegen wollen, und Taste `Enter`.  
*Das Display zeigt `Code-Eingabe, Master ...und Code:`.*
6. Geben Sie den Mastercode ein.  
*Das Display zeigt `Motor Schritt | <== Auf | Zu ==>`.*
7. Wählen Sie mit `<` oder `>` `Auf` oder `Zu`.  
*Das Display zeigt `Bitte warten. Der Riegel fährt einen Schritt auf oder zu, stoppt und das Display zeigt Schritt OK`.*
8. Wiederholen Sie Schritt 7 beliebig oft, wenn gewünscht, auch in Gegenrichtung.

Sie haben den Schlossriegel erfolgreich schrittweise ein- / ausgefahren.

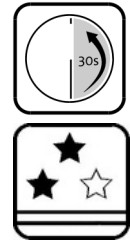
#### 4.15.4 Schloss anmelden

Vorsicht



Verletzungsgefahr für Personen, die nicht fachgerecht montieren sowie Gefahr der Beschädigung und des Funktionsausfalls des Systems.

Stellen Sie sicher, dass geschulte Fachkräfte das System montieren und in Betrieb nehmen.



Mit Menü `Service | Schloss anmelden` können neue, noch nicht adressierte Schlösser angemeldet werden – beim Auswechseln eines Schlosses (`Schloss wechseln`) oder beim Erweitern des Systems um ein Schloss (`Schloss neu`).

Zum Anmelden von Schlössern, die bereits zuvor adressiert worden sind, gehen Sie bitte vor wie beim Wechseln der Bedieneinheit. Siehe Beschreibung „Service Reset“ in diesem Kapitel und die Montageanleitung.

Sie benötigen ein neues, noch nicht adressiertes Schloss

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie `Service` mit Taste `>` und `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Wählen Sie mit `<` oder `>` `Schloss anmelden` und `Enter`.  
*Das Display zeigt `Service | Schloss anmelden`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Schloss anmelden | Schloss neu`.*  
*Weiter geht's bei „Zusätzliches Schloss“ im Fall einer Systemerweiterung oder bei „Schloss wechseln“ beim Wechsel eines Schlosses.*

##### 4.15.4.1 Zusätzliches Schloss

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein zusätzliches neues Schloss anmelden. Siehe auch „Schloss wechseln“ unten.

5. Bestätigen Sie `Schloss neu` mit `Enter`.  
*Das Display zeigt `Code-Eingabe und Systemmanager und Code:`.*
6. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt `Bitte warten | Schloss neu und Schloss 2/3`. Das Display zeigt `! Buskabel ein !`. Die angezeigte Schlossnummer ist die, die das neue Schloss im System bekommt (Anzahl der vorhandenen Schlösser + 1). Wenn Sie das Kabel verbunden haben, bestätigen Sie mit `Enter`.*
7. *Das Display zeigt `Seriennummer | Bitte warten`. Die Seriennummer der Bedieneinheit wird im Schloss gespeichert. Das Display zeigt `Seriennummer | Gespeichert`. Das Display zeigt `Com-Fehler | Setup-Fehler`, wenn das „neue“ Schloss schon einmal adressiert wurde.*

*Das Display zeigt `Datum/Uhrzeit, Gespeichert, Schloss, Angemeldet und TwinLockBusiness | 19.09.23`.*

Sie haben das zusätzliche Schloss erfolgreich angemeldet.

#### 4.15.4.2 Schloss wechseln

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein Schloss auswechseln und das System nicht um ein zusätzliches Schloss erweitern. Siehe auch „Zusätzliches Schloss“ auf Seite 80.

5. Führen Sie Schritte 1-4 der Anleitung „Schloss anmelden“ aus.  
Das Display zeigt *Schloss anmelden | Schloss neu*.
6. Wählen Sie mit < oder > *Schloss wechseln* und Enter.  
Das Display zeigt *Schloss wechseln und Schloss 1<*.
7. Wählen Sie mit < oder > gegebenenfalls das zu ersetzende Schloss und bestätigen Sie mit Enter.  
Das Display zeigt *! Buskabel ein !*.
8. Wenn Sie das Kabel verbunden haben, bestätigen Sie mit Enter.  
Das Display zeigt *Com-Fehler | Setup-Fehler, wenn das „neue“ Schloss schon einmal adressiert wurde*.  
Das Display zeigt *Seriennummer | Schloss 2/3 und Code-Eingabe | Systemmanager, gegebenenfalls 0123456789 und Code:.*
9. Geben Sie den Systemmanagercode ein.  
Das Display zeigt *Seriennummer | Bitte warten. Die Seriennummer der Bedieneinheit wird im Schloss gespeichert*.  
Das Display zeigt *Seriennummer | Gespeichert, Datum/Uhrzeit | Gespeichert, Schloss | Angemeldet und TwinLock Business | 19.09.23*

Sie haben das neue Schloss erfolgreich angemeldet.

### 4.15.5 System bei defektem Riegelwerkskontakt verschließen

Wenn Sie eine Schaltung für einen Riegelwerkskontaktangeschlossen haben, können Sie das System auch bei defektem Schalter einmalig verschließen, indem Sie die im Folgenden beschriebenen Schritte ausführen und dann das System verschließen.

1. Öffnen Sie das Schloss.  
*Siehe in diesem Kapitel Abschnitt „Öffnen und Schließen“.*
2. Drücken Sie kurz **Enter**. Wenn das Display das Datum zeigt, wählen Sie mit der Taste **>Service** und Taste **Enter**.  
*Das Display zeigt Service | Reset.*
3. Wählen Sie mit **> 1x Riegelwerk** und wieder **Enter**.  
*Das Display zeigt Service | 1x Riegelwerk.*
4. Bestätigen Sie mit **Enter**.  
*Das Display zeigt 1x Riegelwerk | \*=Ja \*=Nein.*
5. Wählen Sie mit **>Ja** und danach **Enter**.  
*Das Display zeigt 1x Riegelwerk | Gespeichert.*  
*Sie können das System nun bei defektem Schalter einmalig schließen.*
6. Schließen Sie das Schloss.  
*Siehe die Beschreibungen „Schloss...schließen“. Das System ist gesichert.*



Sie haben das System trotz eines defekten Riegelwerksstellungsschalters erfolgreich verschlossen.

### 4.15.6 Lizenzierung

Menü ist verfügbar ab Firmware Version LP/LQ12. Hier geht es um die Lizenzierung weiterer Software. Softwarelizenzen erhalten Sie auf Anfrage von INSYS Microelectronics.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wenn das Display nichts anzeigt, drücken Sie kurz Taste **Enter**.
3. Wählen Sie mit **> Service** und bestätigen Sie mit **Enter**.  
*Das Display zeigt Service | Reset.*
4. Wählen Sie mit **<** und **> Lizenzierung** und danach **Enter**.  
*Das Display zeigt Code-Eingabe | Systemmanager und Code:.*
5. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt beispielsweise Lizenzierung: 00 und Code: .*  
*Lizenzierung: 00 (Funktionsnummer = 00): Lizenzierung ausgeschaltet.*  
*Bei dieser Einstellung kann die GUI eines Programms angezeigt, aber es kann nicht gespeichert werden. Es werden keine Daten zum Schloss übertragen.*  
*Lizenzierung: 01 ist reserviert für Sondermodelle.*  
*Lizenzierung: FF wird im Fall eines Fehlers angezeigt.*

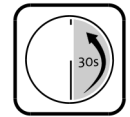


Geben Sie eine 10-stellige Ziffernfolge ohne Leerstellen ein, die aus der 2-stelligen Funktionsnummer (02) und dem 8-stelligen Lizenzierungscode besteht. Die Eingabe von „0000000000“ (Zehn Nullen) löscht die Lizenz gegebenenfalls. Das Display zeigt Gespeichert.

Sie haben die Lizenzierung in / außer Kraft gesetzt.

## Schnell- / Eilsperre in Kraft setzen

Ab Version LP/LQ10 (bei höheren Versionen gegebenenfalls mit anderen als den unten angegebenen Tasten -> Email: support@insys.locks): Für Benutzer, denen ein Wochenprogramm zugeordnet ist, kann das System mit sofortiger Wirkung gesperrt werden.



### Hinweis

Falls beispielsweise mit optionaler PC-Software „Schnellsperre mit Codeeingabe gewählt wurde, ist nach der Wahl von F2 die Eingabe von Benutzer-Nummer und PIN-Code nötig, um die Sperre in Kraft zu setzen.

1. Drücken Sie kurz die Taste Enter.  
*Das Display zeigt Oeffnen oder Schliessen.*
2. Wählen Sie die Taste F2 und, wenn nötig, geben Sie Benutzernummer und Code ein (siehe Hinweis).  
*Das Display zeigt Eilsperre | \*=Ja \*=Nein.*
3. Wählen Sie Ja mit Taste < und danach Taste Enter.  
*Das Display zeigt Eilsperre | Gespeichert.*

Sie haben die Eilsperre für Benutzer, denen ein Wochenprogramm zugeordnet ist, in Kraft gesetzt.

## 4.16 Import / Export

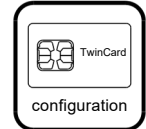
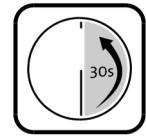
### 4.16.1 Protokollexportieren

Vorbedingungen

Sie sind in der Benutzermatrix Freigabe, Service, PIN-Code (und Chipkarte) aktiviert.  
 Sie benötigen das optionale Parametriererset TwinComm und eine formatierte Chipkarte TwinCard configuration II.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ auf Seite 37.*
2. Wählen Sie mit Menütaste > `Import / Export` und bestätigen Sie mit Taste Enter.  
*Das Display zeigt `Import / Export | Konfiguration`.*
3. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Import / Export | Import`.*
4. Wählen Sie mit der Menütaste > `Export` und `Enter`.  
*Das Display zeigt `Benutzer: Manager | Code-Eingabe`.*
5. Bestätigen Sie mit `Enter` oder wählen Sie mit > und mit `Enter` `Master` oder identifizieren Sie sich als Benutzer.  
*Das Display zeigt `Systemmanager, Master oder Benutzer Nr. und PIN-Code`. Die Eingabe einer Art von Code ist ausreichend.*
6. Bestätigen Sie mit `Enter` und geben Sie PIN-Code ein oder wählen Sie mit > `Codekarte`.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.  
 Das Display zeigt `Bitte warten und danach Daten-Export | Karte ein`.*  
 Stecken Sie Chipkarte TwinCard configuration II in die Eingabeeinheit  
*Siehe „Chipkarte in Bedieneinheit einlegen“ auf Seite 50.*  
*Das Display zeigt `Daten-Export | >>>`.  
 Die Anzahl der Pfeile zeigt den Fortschritt.  
 Die Daten werden auf die Karte geschrieben.  
 Das Display zeigt `Daten-Export | Karte aus`.*
7. 
8. Nehmen Sie die Chipkarte aus der Bedieneinheit.  
*Das Display zeigt `OK` und danach `Import / Export`.*

Sie haben das Protokoll erfolgreich auf Chipkarte gespielt.



## 4.16.2 Protokoll anzeigen / drucken

Öffnungs- und Schließvorgänge, Codeeingaben, Konfigurationsvorgänge und Manipulationsversuche werden protokolliert.

Vorbedingung Protokolldaten wurden bereits auf Karte geschrieben.

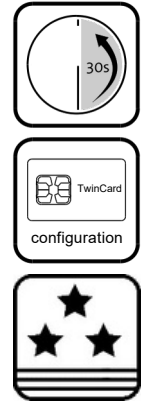
Sie benötigen das optionale Parametrierset TwinComm und die optionale Chipkarte TwinCard configuration II.

1. Starten Sie das Programm TwinComm an Ihrem Computer und wählen Sie die Schaltfläche Protokoll.  
*Registerkarte „Protokoll“ wird am Bildschirm angezeigt.*
2. Stecken Sie die TwinCard configuration II in die Bedieneinheit.
3. Wählen Sie im Fenster TwinComm die Schaltfläche Chipkarte lesen.  
*Am Bildschirm werden die Protokolldaten angezeigt.*  
Falls sich Benutzerdaten seit dem letzten Laden der Karte geändert haben,
4. wählen Sie Schaltfläche Benutzer aktualisieren.  
*Das Protokoll und die aktuellen Benutzerdaten werden angezeigt.*  
Wählen Sie die Schaltfläche mit dem Druckersymbol und die gewünschten Einstellungen, um das Protokoll zu drucken.
5. *Die Protokolldaten werden gedruckt. Mit Schaltfläche*  
*chtern können Sie das Protokoll als CSV-Datei speichern.*

Protokoll spei-

6. Entnehmen Sie die Chipkarte aus der Bedieneinheit.

Sie haben die Protokolldaten erfolgreich angezeigt und gedruckt.

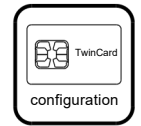
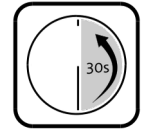


### 4.16.3 Konfiguration importieren

**Vorbedingung** Mit dem optionalen Parametrierset TwinComm ist eine gültige Konfiguration erstellt und gespeichert worden.

Sie benötigen TwinComm und Chipkarte TwinCard configuration II.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ auf Seite 37.*
2. Wählen Sie mit `>Import / Export` und Taste `Enter`.  
*Das Display zeigt `Import / Export | Konfiguration`.*
3. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Import / Export | Import`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe, Systemmanager`, gegebenenfalls `0123456789` und `Code:`.*
5. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt `Bitte warten` und `Daten - Import | Karte ein`.*
6. Legen Sie die Karte TwinCard configuration II in die Bedieneinheit.  
*Siehe Abschnitt „Chipkarte in Bedieneinheit einlegen“ auf Seite 50.  
Das Display zeigt `1 >>> 5`. Die Konfiguration wird importiert. Falls sie nicht zulässige Parameter enthält, werden Fehlermeldungen angezeigt. Siehe die folgende Meldungsliste. Das Display zeigt `5 >>> 5` und `Daten - Import | Karte aus`.*
7. Nehmen Sie die Chipkarte aus der Bedieneinheit FlatControl.



Sie haben das System erfolgreich konfiguriert.

#### 4.16.4 Meldungen beim Import der Konfiguration

Beim Import einer Konfiguration können die im Folgenden aufgelisteten Meldungen angezeigt werden, wenn das System Konfigurationsfehler diagnostiziert.

- Ändern Sie ungültige Parameter mit der Bedieneinheit beziehungsweise mit der optionalen PC-Software und lesen Sie die Konfiguration erneut ein.

In der ersten Zeile des Displays können angezeigt werden:

Schlosssystem. bei einem Parameter mit ungültigem Wert und  
In der zweiten Zeile des Displays können angezeigt werden:  
Alarmverzögerung bei nicht zum System passender Konfiguration

- ! Alarmverzögerung bei stillem Alarm liegt nicht im zulässigen Wertebereich von 0-99 Minuten.  
✓ Tragen Sie einen zulässigen Wert ein.

Alter Code

- ! Der Wert für „Codealterung“ liegt nicht im zulässigen Wertebereich von 0-12 Monaten.  
✓ Tragen Sie einen zulässigen Wert ein.

Benutzer neu

- ! Die Benutzernummer, der Einmalcode zugeordnet wurde, liegt nicht im zulässigen Bereich von 0-99 / 225 (Manager).  
✓ Tragen Sie einen zulässigen Wert ein.

Öffnen

- ! Der bei Parameter „Öffnung Schloss 1 -> 2“ eingegebene Wert liegt nicht im zulässigen Wertebereich von 00-99 Minuten.  
✓ Tragen Sie einen zulässigen Wert ein.

Parallelcode

- ! „Parallelcode“ und „4-Augen-Prinzip (Öffnung)“ sind gleichzeitig aktiviert.  
✓ Deaktivieren Sie eine der Optionen.

PIN-Codes

- ! Zu wenig PIN-Codes im System. Falls die Konfiguration importiert würde, könnte das System nicht geöffnet werden.  
✓ Erhöhen Sie die Anzahl berechtigter Benutzer im System und melden Sie PIN-Codes für sie an.

Schließen & Code

- ! „Schliessen mit Code“ und „Automatisches Schliessen“ / „Öffnung Schloss 1 -> 2“ sind aktiviert.  
✓ Deaktivieren Sie eine der Optionen.

**Sondertage**

- ! Für mindestens einen „Sondertag“ wurde ein ungültiges Datum eingetragen.
- ✓ *Berichtigen Sie die Daten für „Sondertage“.*

**Sperrzeit**

- ! Für Zeitprogramm „Sperrzeit“ wurde mindestens ein ungültiges Datum eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Stiller Alarm**

- ! Der Wert für „Alarmziffer“ in der PC-Software liegt nicht im zulässigen Wertebereich von 01-09.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Teilsperrezeit**

- ! Für Zeitprogramm „Teilsperrezeit“ wurde mindestens eine ungültige Uhrzeit eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Tuer offen**

- ! Der Wert für „Türöffnungsüberwachung“ liegt nicht im zulässigen Wertebereich von 00-99 Minuten.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**TwinAlarm**

- ! Sowohl TwinXT (II) / TwinXT small als auch TwinAlarm sind aktiviert.
- ✓ *Deaktivieren Sie das Gerät, das nicht im System ist.*

**Wochenprogramm**

- ! Für Zeitprogramm „Wochenprogramm“ wurde mindestens eine ungültige Uhrzeit eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**WTU-Benutzer**

- ! Die Benutzernummer des ersten „WTU-Benutzers“ liegt nicht im zulässigen Wertebereich von „01-99“.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

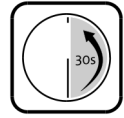
**Zeitverzögerung**

- ! Der Wert für „Öffnungsverzögerung“ eines Schlosses liegt nicht im zulässigen Wertebereich von 00-99.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

### 4.16.5 Konfiguration exportieren

Sie können die Konfiguration des Schlosssystems über Chipkarte in die Parametriersoftware TwinComm exportieren.

Sie benötigen das optionale Parametrierset TwinComm und die optionale Chipkarte TwinCard configuration II.



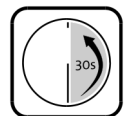
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Menütaste `>` `Import / Export` und bestätigen Sie mit `Enter`.  
*Sie befinden sich im Menü `Import / Export`.  
Das Display zeigt `Import / Export | Konfiguration`.*
3. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Import / Export | Import`.*
4. Wählen Sie mit `>Export` und `Enter`.  
*Das Display zeigt Code-Eingabe, Systemmanager, gegebenenfalls `0123456789` und Code:. Aus der Anzeige ist ablesbar, wie der Code einzugeben ist. Siehe Abschnitt „PIN-Code eingeben“.*
5. Geben Sie den Systemmanagercode ein.  
*Danach zeigt das Display `Bitte warten` und `Daten - Export | Karte ein`.*
6. Legen Sie Karte TwinCard configuration II in die Bedieneinheit.  
*Siehe auch Abschnitt „Chipkarte in Bedieneinheit einlegen“.  
Das Display zeigt `>>>`. Die Anzahl der Pfeile zeigt den Fortschritt.  
Die Daten werden auf die Chipkarte geschrieben.  
Das Display zeigt `Daten - Export | Karte aus`.*
7. Nehmen Sie Ihre Chipkarte aus der Eingabeeinheit.

Sie haben die Konfiguration erfolgreich auf die Chipkarte gespielt.

### 4.16.6 Sprache wählen

Jeder Benutzer kann aus drei Sprachen auswählen, wenn diese vorher in der Bedieneinheit gespeichert wurden.

1. Wählen Sie mit den Menütasten `Import / Export` und `Enter`.  
*Das Display zeigt `Import / Export | Konfiguration`.*
2. Wählen Sie mit `>Sprache` und bestätigen Sie mit `Enter`.  
*Das Display zeigt beispielsweise `Sprache | 1 Deutsch`. Sie können die Sprache auf Sprachplatz 1, 2 oder 3 wählen. Die gewählte Sprache wird im Folgenden mit `gewählte Sprache` bezeichnet.*
3. Wählen Sie eine Sprache mit `>` und Taste `Enter`.  
*Das Display zeigt `Gewählte Sprache | Gespeichert` und danach `OK`.*



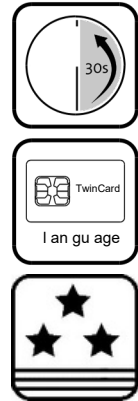
Sie haben die Sprache des Displays von FlatControl erfolgreich geändert.

### 4.16.7 Sprache importieren

Die Bedieneinheit verfügt über drei Sprachplätze, auf denen drei Sprachen gespeichert werden können.

Sie benötigen die optionale Chipkarte TwinCard language (v2.xx).

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Menütaste `> Import / Export` und `Enter`.  
*Das Display zeigt `Import / Export | Konfiguration`.*
3. Wählen Sie mit `> Sprache` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Sprache | 1 Deutsch`.*
4. Wählen Sie mit `> Daten-Import` und `Enter`.  
*Das Display zeigt `Sprache | Daten-Import`, danach `Code-Eingabe`,  
`Systemmanager, ...` und `Code: .`*
5. Geben Sie den Systemmanagercode ein.  
*Danach zeigt das Display `Sprache | Bitte warten` und `Sprache | Sprachplatz 1<`. Der Cursor blinkt.*
6. Wählen Sie mit `>` den Sprachplatz und danach `Enter`.  
*Falls vorher eine andere Sprache diesen Sprachplatz hatte, wird sie gelöscht.  
Das Display zeigt `Sprache Import | Karte ein`.  
Stecken Sie die Chipkarte TwinCard language in die Bedieneinheit.*
7.  
*Das Display zeigt `Daten - Import | Sprache und >>>> ..Die Daten werden importiert. Das Display zeigt Daten - Import | Karte aus.`*
8. Nehmen Sie die Chipkarte aus der Bedieneinheit.



Sie haben erfolgreich eine Sprache importiert.

## 5 Wartung, Reparatur und Reinigung

Das System ist wartungsfrei. Es wurde vor Auslieferung auf 100.000 Öffnungs- und Schließzyklen geprüft.

Der vom Hersteller des Riegelwerks angegebene Wartungszyklus ist für das Riegelwerk einzuhalten.

Reparaturen dürfen ausschließlich von Elektrofachkräften (siehe Definition auf Seite 12), die von INSYS MICROELECTRONICS oder berechtigten Partnerunternehmen geschult und autorisiert wurden, durchgeführt werden.

### Vorsicht

Gefahr von Kurzschluss der elektronischen Komponenten.

Gefahr der Beschädigung des Systems

Beachten Sie die Anweisungen zur Reinigung des Systems.

Reinigen Sie die Eingabeeinheit mit sehr wenig Wasser oder mit sehr wenig milder Seifenlösung. Verwenden Sie dazu ein feuchtes, weiches, sauberes und fusselfreies Tuch. Verwenden Sie keine anderen Mittel. Verwenden Sie zur Desinfektion (Wischdesinfektion, Nachwischen mit einem mit Trinkwasser befeuchtetem Tuch) nur Mittel, deren Produktbeschreibung ausweist, dass sie über eine gute Materialverträglichkeit mit den Kunststoffen Polyethylen (PE), ABS und PC-ABS verfügen.

Reinigen Sie alle anderen Komponenten des Systems TwinLock nur, wenn Ihnen dies unumgänglich erscheint. Benutzen Sie ausschließlich ein trockenes, weiches, sauberes und fusselfreies Tuch.

Wischen Sie über die Oberfläche, ohne großen Druck auszuüben.

## 6 Störungsabhilfe

### 6.1 System bei Netzausfall mit Spannung versorgen

Batteriehersteller bieten passende 9 Volt Blockbatterien unter den Bezeichnungen 6LR61 (Alkali-Mangan), 6F22 (Zink-Kohle), 6AM6, 522 an.

Sie benötigen ein Adapterkabel (im Lieferumfang), eine aufgeladene 9 Volt Blockbatterie und Zugriff auf die Bedieneinheit.

1. Verbinden Sie Adapterkabel und Batterie. Achten Sie dabei auf die unterschiedliche Größe der Steckverbindungen von Plus- und Minuspol der Batterie.
2. Stecken Sie den Mini DC-Stecker des Adapterkabels in die Buchse auf der Unterseite der Bedieneinheit.

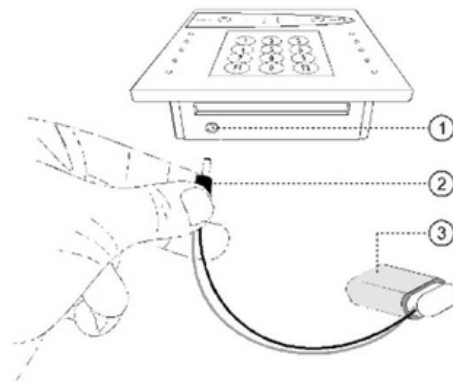


Abb. 22: Adapterkabel mit Eingabeeinheit verbinden

- 1) Buchse für Spannungsversorgung bei Netzausfall
- 2) Mini DC-Stecker des Adapterkabels
- 3) 9 Volt Blockbatterie

Sie versorgen das System erfolgreich mit Spannung.

### 6.2 Fehlermeldungen

Siehe auch Kapitel „Bedienung“, Abschnitt „Meldungen beim Einlesen der Konfiguration“.

#### Alarm-Codefehler

- ! Fehler beim Speichern eines Codes in TwinAlarm.
- √ *Wiederholen Sie den Speicherungsversuch. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung wiederholt angezeigt wird.*

#### Autorisierung

Codekarte Freigabe Öffnen PIN-Code Schließen & Code Service  
Unschärfen Schalten

!

Benutzer ist für den gewählten Vorgang nicht autorisiert. Nach einer Sekunde zeigt das Display, welche Art der Autorisierung dem Benutzerin der Benutzermatrix der PC-Software nicht verliehen wurde (siehe unten, „Codekarte“, „Freigabe“...).

√

*Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, damit die Autorisierung in der Benutzerverwaltung von TwinComm ergänzt.*

**Codekarte**

- ! Benutzer darf keine Codekarte benutzen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Keine Freigabe**

- ! Benutzer hat keine Freigabe für die Eingabe von Codes.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Öffnen**

- ! Benutzer darf kein Schloss öffnen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**PIN-Code**

- ! Benutzer darf keinen PIN-Code eingeben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Schließen&Code**

- ! Benutzer darf Schlösser mit der Eingabe von PIN-Code nicht schließen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Service**

- ! Benutzer darf Protokoll nicht exportieren.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Unscharfschalten**

- ! Benutzer darf Einbruchmeldeanlage nicht „unscharf“ schalten. Behebung siehe oben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Bus A/B empfangen****Bus A/B senden**

- ! Ein Schloss lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

**Codes identisch!**

- ! Ein neuer Code entspricht dem bisherigen, zu ändernden.
- ✓ *Melden Sie einen anderen Code an.*

**COM-Fehler****Fehler Antwort**

- ! In der Kommunikation zwischen der Bedieneinheit und einer anderen Systemkomponente (z.B. einem Schloss) ist ein Fehler aufgetreten. Die Bedieneinheit hat einen nicht vorgesehenen Befehl empfangen.
- ✓ *Softwarefehler. Setzen Sie sich bitte mit dem Support in Verbindung.*

## COM-Fehler

## Bus A/B senden Bus A/B empfangen

- ! Ein Schloss lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

## EEPROMfehler AB / DMS / TM

- ! Fehler beim Lesen vom / Schreiben ins EEPROM der Bussysteme (AB) / von Schloss (DMS) / der Bedieneinheit (TM für Terminal).
- ✓ *Wiederholen Sieden Vorgang. Setzen Siesich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

## Eingabefehler

- ! Falsche / ungültige Eingabe. Möglicherweise wurde ein PIN-Code nicht korrekt eingegeben oder bei gewählter Option „Parallelcode“ oder „Codeverknüpfung“ haben nicht zwei verschiedene Benutzer ihren Code eingegeben, sondern nur einer.
- ✓ *Wiederholen Sieden Vorgang. Setzen Siesich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

## Falscher Code | Sperrzeit

- ! Beim Versuch, ein Schloss zu öffnen, wurde beispielsweise viermal (Software-Einstellung, beispielsweise via TwinComm) ein falscher Code eingegeben, wodurch eine Sperrzeit aktiviert wurde. Die Sperrzeit verlängert sich bei jeder weiteren Falscheingabe um eine Minute.
- ✓ *Warten Sie ab, bis die Sperrzeit abgelaufen ist, und geben Sieden Code korrekt ein.*
- ✓ *Setzen Sie sich bitte mit Ihrem Systemadministrator / dem Support in Verbindung, wenn Sie nicht im Besitz des korrekten Codes sind.*

## Falsche Karte

- ! Ein Benutzer hat eine Karte des falschen Typs in die Bedieneinheit gesteckt, beispielsweise eine Sprach- statt einer Konfigurationskarte.
- ✓ *Wählen Sie die passende Karte. Setzen Siesich bitte mit dem Support in Verbindung, wenn Sie nicht im Besitz der geeigneten Karte sind.*

## Fehler DMS Nr.

- ! Das Schloss mit der angegebenen Nummer meldet einen allgemeinen Fehler.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

## Fehler Karte

- ! In der Kommunikation zwischen der Bedieneinheit und einer Chipkarte ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sieden Vorgang. Setzen Siesich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

## Fehler Motor A

## Fehler Motor B

- ! Der Riegel des Schlosses kann nicht über Bus A / Bus B bewegt werden. Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

**Fehler Scharf!**

- ! TwinAlarm meldet Fehler beim Scharfschalten der Einbruchmeldeanlage (EMA): EMA kann nicht scharf geschaltet werden, weil das System nicht gesichert ist.
- ✓ *Schließen Sie die Schlösser und wiederholen Sie den Vorgang.*

**Fehler: Seriennr.**

- ! Die Seriennummern in der Bedieneinheit und im Schloss sind nicht identisch.
- ✓ *Diese Meldung wird angezeigt, wenn Bedieneinheit oder Schloss nicht vorschriftsmäßig gewechselt wurden. Sabotage ist möglich. Bitte setzen Sie sich mit den für die Sicherheit zuständigen Personen in Verbindung.*

**Fehler TwinAlarm**

- ! In der Kommunikation mit der Schalteinrichtung TwinAlarm ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sieden Vorgang. Setzen Siesich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Fehler Unscharf!**

- ! TwinAlarm meldet Fehler beim Unscharf-Schalten der Einbruchmeldeanlage (EMA): EMA kann nicht unscharf geschaltet werden, weil von ihr keine Quittierung der Unscharf-Schaltung erfolgt.
- ✓ *Setzen Siesich bitte mit dem Alarmtechniker / Support in Verbindung, um die Verbindung zur EMA überprüfen zu lassen.*

**Keine Freigabe**

- ! Keine Öffnung möglich. Schloss ist über den Eingang FREIGABE von TwinXT (II, small) / TwinAlarm nicht freigegeben.
- ✓ *Prüfen Sie, ob TwinXT (II, small) / TwinAlarm richtig angeschlossen ist und ob das Schloss berechtigterweise gesperrt ist. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung weiterhin angezeigt wird.*

**Keine Karte**

- ! Es wurde keine Chipkarte in die Bedieneinheit eingelegt.
- ✓ *Legen Sie eine Chipkarte in das Kartenfach unten in der Bedieneinheit.*

**Keine TwinAlarm!**

- ! Die Schalteinrichtung TwinAlarm ist deaktiviert.
- ✓ *Stellen Sie sicher, dass die Schalteinrichtung richtig angeschlossen und initialisiert ist.*

**! Manipulation !**

- ! Ein Code wurde mehr als dreimal falsch eingegeben.
- ✓ *Kontrollieren Sie im Protokoll, welcher Benutzer dies verursacht hat.*

**Motorfehler**

- ! Der Riegel des Schlosses kann nicht bewegt werden. Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition wegen eines mechanischen Problems nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

Neustart | stromlos siehe stromlos

#### RTC-Fehler

- ! Die Uhr (Real Time Clock) der Bedieneinheit funktioniert nicht korrekt.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

#### Schloss Mitte

- ! ✓ Schlossriegel ist weder geschlossen noch geöffnet, sondern in Mittelposition.
- ✓ *Prüfen Sie, ob sich ein Hindernis vor dem Schlossriegel befindet, welches das Ausfahren des Riegels behindert.*
- Prüfen Sie, ob sich das Schloss öffnen / schließen lässt. Wenn nicht, setzen Sie sich bitte mit dem Support in Verbindung.*

#### Schlosssystem

- ! Es wurde versucht, einen Code abzumelden, ohne den das System nicht mehr zu öffnen wäre.
- ✓ *Deaktivieren Sie gegebenenfalls „Codeverknüpfung“ oder „Parallelcode“ oder ordnen Sie die Öffnungsberechtigung für das Schloss weiteren Benutzern zu, bevor Sie den Code abmelden.*

#### Sondertage

- ! ✓ Das aktuelle Datum fällt auf einen „Sondertag“, an dem das Öffnen des Schlosses nicht gestattet ist.
- ✓ *Warten Sie, bis der „Sondertag“ vorbei ist.*
- ✓ *Öffnen Sie das Schloss (mit Autorisierung zur Schnellöffnung).*
- Prüfen Sie das an der Eingabeeinheit FlatControl eingestellte Datum und korrigieren Sie es gegebenenfalls.*

#### Sperrzeit (siehe auch „Falscher Code | Sperrzeit“)

- ! Beim Versuch, das Schloss zu öffnen,
  - wurde mehrmals ein falscher Code eingegeben
  - wurde eine Sperrzeit von 90 Minuten aktiviert, weil mindestens ein Schloss während eines Terminalwechsels geschlossen
  - wurde versucht, das Schloss während eines Sperrzeitraums zu öffnen.
- ✓ *Warten Sie, bis die Sperrzeit abgelaufen ist und geben Sie den korrekten Code ein.*
- ✓ *Lassen Sie anhand des Protokolls / vom für die Sicherheit zuständigen Personal prüfen, ob versucht wurde, am System zu manipulieren.*

#### stromlos

- ! Das System war getrennt von der Stromversorgung. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Prüfen Sie, ob Datum und Uhrzeit richtig eingestellt sind.*
- ✓ *Überprüfen sie das Protokoll.*
- ✓ *Lassen Sie vom für die Sicherheit zuständigen Personal prüfen, ob am System manipuliert wurde.*

**Terminal-Wechsel**

- ! Bedieneinheit wurde gewechselt oder zurückgesetzt. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Diese Meldung erfolgt beim ersten Öffnungs-/Schließvorgang nach dem Zurücksetzen (Reset) oder nach dem Wechsel der Bedieneinheit. Sie erfordert keine Maßnahmen.*
- ✓ *Wenn die Meldung unerwartet erfolgt, könnte es sich um einen Manipulationsversuch handeln. Setzen Sie sich in diesem Fall bitte mit dem für die Sicherheit zuständigen Personal in Verbindung.*

**trivialer Code**

- ! Ein Benutzer hat einen Code eingegeben, der aus einer Folge auf - , absteigender - oder gleicher Ziffern besteht.
- ✓ *Aus Sicherheitsgründen kann eingestellt werden, dass solche Codes nicht erlaubt sind. Geben Sie einen anderen Code ein.*

**ungültige Karte**

- ! Die Codekarte ist ungültig.
- ✓ *Prüfen Sie, ob Sie eine gültige Karte haben. Setzen Sie sich bitte mit dem Systemadministrator / dem Support in Verbindung, wenn Sie keine gültige Karte besitzen.*

**Unscharf-Code??**

- ! TwinAlarm kann die angeschlossene Einbruchmeldeanlage (EMA) nicht scharf schalten, weil noch kein Code zum Unscharf-Schalten angemeldet wurde.
- ✓ *Aktivieren Sie gegebenenfalls TwinAlarm und melden Sie einen Code zum Unscharf-Schalten an.*

**War Neustart oder | stromlos**

- ! Das System war getrennt von der Stromversorgung. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Prüfen Sie, ob am System manipuliert wurde und ob Datum und Uhrzeit richtig eingestellt sind.*

**Wochenprogramm**

- ! Die aktuelle Uhrzeit liegt nicht innerhalb eines mit der Funktion „Wochenprogramm“ definierten Zeitfensters für die Öffnung des Schlosses.
- ✓ *Warten Sie, bis das Zeitfenster für die Öffnung kommt.*
- ✓ *Lassen Sie das Schloss von einem via Benutzermatrix in TwinComm zur „Schnellöffnung“ autorisierten Benutzer öffnen.*
- ✓ *Prüfen Sie das an der Bedieneinheit eingestellte Datum und korrigieren Sie es gegebenenfalls.*

**Zeitprog. Abbruch**

- ! Statusmeldung. Die Schaltung Zeitprogramm Sperre im gesicherten Bereich Ihres Systems ist geschlossen und unterbricht alle aktiven Zeitprogramme oder ein zur „Schnellöffnung“ autorisierter Benutzer hat ein Schloss trotz aktiven Zeitprogramms geöffnet.
- ✓ *Wenn Sie nicht wünschen, dass aktive Zeitprogramme unterbrochen werden, öffnen Sie die Schaltung Zeitprogramm Sperre.*

## 7 Technische Unterstützung

INSYS MICROELECTRONICS GmbH  
Hermann-Köhl-Sr. 22  
93049 Regensburg, Germany

Telefon: +49 941 58692 220  
Telefax: +49 941 58692 45  
E-Mail: support@insys-locks.de  
Internet: http://www.insys-locks.com

8 Entsorgen Sie Plastik-, Elektronikteile und Kabel, indem Sie sie zu einem zertifi-

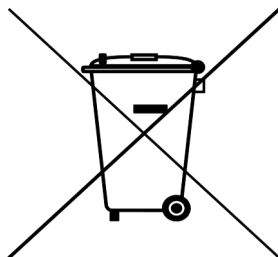
zierten Entsorgungsfachbetrieb in Ihrer Nähe bringen oder sie an diese Adresse senden:



Frankenberg – Metallrecycling GmbH  
Industriestr.1  
D 91448 Emskirchen

Telefon: +49 9104 82622-0  
Telefax: +49 9104 82622-22  
E-Mail: anfrage@fmr.ag  
Internet: http://www.frankenberg-metallhandel.de

Senden Sie Schlösser, gekennzeichnet als „zur Entsorgung“, für eine ordnungsgemäße Rücknahme und Verwertung an diese Adresse:



INSYS MICROELECTRONICS GmbH  
Hermann-Köhl-Str. 22  
93049 Regensburg, Deutschland

## 9 Glossar

Bei Begriffen, die wie Anmelden im Fließtext fettgedruckt sind, handelt sich um Begriffe, zu denen es eigene Einträge im Glossar gibt.

Um die Lesbarkeit nicht zu sehr zu beeinträchtigen, sind nur ausgewählte Begriffe fett gedruckt, die im jeweiligen Kontext eine wichtige Rolle spielen. Lesen Sie auch die Einträge zu diesen Begriffen.

Alle Einträge sind in alphabetischer Reihenfolge aufgeführt.

4-Augen-Prinzip (Öffnung / Konfiguration / Schließen / Freigabe)  
siehe Codeverknüpfung.

Abmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer das Schloss mit diesen Codes öffnen können. Wenn

der

Schlossmaster einen PIN-Code / eine Codekarte an einem Schloss abmeldet, kann der zugehörige Benutzer diese nicht mehr verwenden.

Alarmcode (für Stillen Alarm)

Aktiviert Stillen Alarm und berechtigt zu den gleichen Aktionen wie der zugehörige PIN-Code von Schlossmaster oder (Standard-)Benutzer.

PIN-Code, dessen letzte Ziffer um den in der Software TwinComm gesetzten Wert für Alarmcode erhöht ist.

Ist beispielsweise die letzte Ziffer Ihres PIN-Codes 9, geben Sie als letzte Ziffer des Alarmcodes die Ziffer „9+eingetragener Wert“ ein. Wenn das Ergebnis dieser Addition zweistellig ist, übertragen Sie nur die zweite Stelle als letzte Codeziffer, beispielsweise nach  $9 + 1 = 10$  als letzte Codeziffer „0“.

Anmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer sie verwenden können.

Autorisierung

bedeutet hier das, welche Rechte der Systemmanager für Benutzer des Schloss-Systems in der Benutzermatrix und für Benutzergruppen in Bereich „Einstellungen“ der PC-Software festlegt. Siehe auch Kapitel „Bedienung“, Abschnitt „Bedienung/Benutzer-Autorisierung“.

Autorisierung zum Öffnen eines Schlosses

Ein Benutzer hat das System so konfiguriert, dass er z.B. ein Schloss öffnen kann, wenn er autorisiert hat (siehe Kapitel „Bedienung“, Abschnitt „Benutzer autorisieren“) und

- wenn der Schlossmaster für ihn an diesem Schloss PIN-Code und / oder Codekarte (passend zur Autorisierung) angemeldet hat und
- wenn aktuell kein Zeitprogramm das Öffnen unterbindet.

Optional kann das System so konfiguriert werden, dass nur zwei Personen gemeinsam oder zeitlich versetzt ein Wertbehältnis öffnen können (siehe auch Codeverknüpfung Parallelcode).

Benutzergruppen

### Vorsicht

Ohne autorisierten WTU-Master kann der WTU-Benutzerbereich nicht verwaltet werden.

Autorisieren Sie Benutzer 99 vor Aktivierung von „Benutzergruppen“ ausreichend.

Bei aktivierter Option „Benutzergruppen“ werden die Benutzer jedes Schlosses im System in zwei Gruppen aufgeteilt. Der neue Benutzerbereich bekommt Benutzer Nr.99, der zum „WTU-Master“ wird, als Verwalter. Der ursprüngliche Benutzer-

bereich verkleinert sich um den neuen Bereich. Die Größe der Gruppen kann fest eingestellt / über das optionale Parametrierset TwinComm definiert werden. Für die Bedienung mit Benutzergruppen kann beispielsweise über Feld „Öffnung

Be-

nutzergruppen zwingend“ (wird nur angezeigt, wenn Feld „WTU/2 Ben.-Gruppen aktiv“ markiert) auf Registerkarte „Einstellungen“ von TwinComm eingestellt werden, ob die Gruppenmitglieder bei „4-Augen-Prinzip (Öffnung)“ oder „Parallelcode“

- nur gemeinsam mit Mitgliedern ihrer Gruppe (Wert: „gleich“) oder
- nur mit einem Mitglied der anderen Gruppe (Wert: „verschieden“) oder
- mit einer Person aus irgendeiner Gruppe (Wert: „keine“) öffnen können.

Die erste Benutzergruppe (Benutzer Nr.01 bis zu Benutzer Nr.XX-1) wird nach wie vor vom Schlossmaster verwaltet. Die neue Gruppe der WTU-Benutzer von Benutzer Nr.XX (= frei definierbare Nr. zwischen 1 und 98) bis Nr.98 wird von Benutzer Nr.99, dem WTU-Master verwaltet.

Benutzermatrix

Registerkarte in PC-Software, auf der die individuellen Benutzerrechte festgelegt werden; siehe Kapitel Bedienung, Abschnitt „Benutzer-Autorisierung“.

Benutzern können unter anderem Personalnummern zugeordnet werden.

Code

steht hier für geheime Daten, die ein Benutzer dem System übermitteln muss, bevor er Schlösser öffnen / gegebenenfalls schließen und anderes ausführen darf. Kann

als

PIN-Code und gegebenenfalls zusätzlich als OTC und via Codekarte übermittelt werden.

Codealterung

Gültig für PIN-Code. Einstellbar von 00-12 Monate, 00 Monate = deaktiviert

Wenn die Option aktiviert ist, wird jeder PIN-Code bei jedem Öffnungsversuch eines Schlosses auf den Zeitpunkt seiner Anmeldung geprüft.

Wenn der Code vor längerer Zeit als dem eingestellten Intervall angemeldet wurde, muss der Benutzer den Code ändern. Ab Firmware LP/LQ14 gibt es 3 Arten der Alterung.

Codekarte

Chipkarte TwinLock code access oder RFID-Karte. Trägermedium von Code, Ergänzung zur Eingabe von PIN-Code.

## Codeverknüpfung

4-Augen-Prinzip (Öffnung / Konfiguration / Schließen / Freigabe / ...)

Wenn dasentsprechende Kontrollkästchen markiertist,ist

- die Öffnung von Schlössern,
- die Systemkonfiguration,
- das Schließen von Schlössern beziehungsweise
- die Code-Eingabe während der Freigabezeit

nur möglich, nachdem sich zwei Benutzer am selben Schloss authentifiziert haben.

„4-Augen-Prinzip (Öffnung)“ ist nicht zusammen mit Parallelcode möglich. Ausgewählte Benutzer können über die Benutzermatrix dazu berechtigt werden, trotz „Dualcode / 4-Augen-Prinzip (Öffnung)“ Schlösser auch allein zu öffnen.

Werkseinstellung: nicht aktiviert.

## Echtzeituhr

Datum und Uhrzeit werden von einer speziell gepufferten Echtzeituhr generiert und bleiben im Notfall auch trotz mehrtägiger Stromlosigkeit des Systems aktuell.

Wird die Bedieneinheit für längere Zeit von der Stromversorgung getrennt, müssen Systemzeit und Datum neu eingegeben werden. Die automatische Sommer- / Winterzeitumstellung ist werksseitig voreingestellt. Sie kann via PC-Software ausgeschaltet werden.

## Einmalcode (OTC)

Code für Benutzer, der nach einmaliger Verwendung ungültig wird. Zuordenbar via PC-Software. Unabhängig von Option WTU / Benutzergruppen.

## Fester Code

Optionale Einstellung, kein Standard. Einstellung, dass Benutzer ihren PIN-Code nicht selbständig ändern können. In der Benutzermatrix gegebenenfalls zuordenbar.

## Freigabezeit

Die Freigabezeit können Sie mit der optionalen PC-Software für jedes Schloss auf eine Dauer von 1-99 Minuten festlegen.

Für jedes Schloss können Sie mit TwinComm eine Öffnungsverzögerung programmieren, während der das Schloss nach der Code-Eingabe eines Benutzers noch geschlossen bleibt.

Bei aktivierter Option „Freigabezeit“ muss der Benutzer nach Ablauf der Öffnungsverzögerung seinen Code während der sogenannten Freigabezeit erneut übermitteln, damit sich das Schloss öffnet.

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

## Managercode

### Vorsicht

Mit werksseitigem Systemmanagercode ist die Konfiguration Ihres Systems nicht gesichert.

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.225 (Manager) zugeordneten Managercode, der im Schloss gespeichert ist und nicht abgemeldet werden kann. Der Managercode des Schlosses 1, des Systemschlusses, berechtigt dazu, Systemeinstellungen zu machen und wird daher auch als Systemmanagercode und kurz als Systemcode bezeichnet. Werksseitig ist der Managercode eines jeden Schlosses als Code „111111“ (bei Systemen der VdS Klasse 2) oder „11111111“ (bei Systemen der VdS Klasse 3) programmiert.

## Mastercode

## Vorsicht

Mit werksseitigen Mastercodes ist Ihr System nicht gesichert.

Ändern Sie werksseitige Codes bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.00 (Schlossmaster) zugeordneten Mastercode, der im Schloss gespeichert ist und nicht abgemeldet werden kann. Der Mastercode berechtigt dazu, Schlossbenutzer zu verwalten. Werksseitig ist der Mastercode für Schlösser der VdS Klasse 2 als Ziffernfolge „123456“ und für Schlösser der Klasse 3 als „12345678“ programmiert. In der Benutzermatrix der optionalen PC-Software TwinComm kann der Systemmanager festlegen, ob der Mastercode auch zur Öffnung des Schlosses berechtigt.

## Menütasten

FlatControl: Vier Tasten, CLEAR, <, > und ENTER, die sich direkt unter dem Display der Bedieneinheit befinden.

Die Tasten dienen jeweils zur Navigation in den angezeigten Menüs und zur Auswahl von Eingabewerten.

## Netzausfall

Um Schlösser auch bei Netzausfall öffnen und schließen zu können, wenn das System über ein Netzteil (Netzteilbetrieb über TwinConnect / TwinConnect small) versorgt wird, schließen Sie eine 9 Volt Blockbatterie Typ Alkaline an der Bedieneinheit an. Stecken Sie das Adapterkabel in die Buchse an der Unterseite der Bedieneinheit. Siehe Abschnitt „System während Netzausfall mit Spannung versorgen“.

## Öffnungsverzögerung

Für jedes Schloss können Sie mit der optionalen PC-Software TwinComm eine Öffnungsverzögerung von 1-99 Minuten programmieren. Für diesen Zeitraum bleibt das Schloss auch nach der Code-Eingabe des Benutzers geschlossen. Siehe auch Option

## Freigabezeit

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

## Öffnungszeit

Siehe Sperrzeit / Öffnungszeit (Zeitprogramm).

## Parallelcode

Nur möglich bei Systemen mit mindestens zwei Schlössern. Der erste Benutzer kann Schloss 1, 2 oder 3 öffnen, der zweite gegebenenfalls eines der beiden noch geschlossenen und der dritte das letzte.

Kombinierbar mit „Zwangsfolge“. Wenn 2 Schlösser im System sind, kann ein Benutzer während einer „Teilsperrezeit“ ein Wertbehältnis auch alleine öffnen.

Bei Aktivierung dieser Funktion mit dem optionalen Parametrierset TwinComm wird die Funktion „Codeverknüpfung“ automatisch deaktiviert.

## Personalnummern

Benutzern können Personalnummern zugeordnet werden und über ein Kontrollkästchen in der Benutzermatrix der PC-Software kann definiert werden, ob sich alle Benutzer mit ihren Personalnummern statt mit ihren Benutzernummern identifizieren.

## PIN-Code

Persönliche Identifikationsnummer (PIN) oder Geheimzahl, die Benutzer an der Bedieneinheit eingeben. Eine nur einem oder einem Benutzer und dem Schlossmaster bekannte Ziffernfolge, mit der Benutzer sich gegenüber System TwinLock authentifizieren können.

**Protokoll (Ereignisprotokoll)**

Alle wichtigen Ereignisse werden mit Datum / Uhrzeit chronologisch protokolliert und können gegebenenfalls online übertragen werden. Beteiligte Geräte und Benutzer werden aufgeführt. Die jüngsten 3000 (TwinComm) werden im Protokoll gespeichert. Ereignisse sind Programmiervorgänge, Systemfehler, kritische Statusmeldungen sowie Manipulations- und Sabotageversuche. Der gesamte Ereignisspeicher kann auf Chipkarte TwinCard configuration II gespielt und mit der PC-Software TwinComm angezeigt und gedruckt werden.

**Schlossmaster**

Inhaber des Mastercodes eines Schlosses, der die Codes (PIN-Codes und Codekarten) der Benutzer dieses Schlosses verwaltet. Ob der Schlossmaster das Schloss selbst öffnen kann, ist abhängig davon, was der Systemmaster in der Benutzermatrix einstellt. Siehe auch Benutzergruppen.

**Schnellöffnung**

Kontrollkästchen in der Benutzermatrix der optionalen Software TwinComm. Wenn es markiert ist, kann ein Benutzer ein Schloss trotz programmierter Zeitprogramme öffnen, ohne warten zu müssen.

Dazu müssen für ihn auch alle anderen für die Autorisierung zur Schlossöffnung nötigen Kästchen markiert und sein PIN-Code muss am Schloss angemeldet worden sein.

**Service**

1) Menü im Display der Bedieneinheit für Servicefunktionen

2) Kontrollkästchen in der Benutzermatrix der PC-Software. Wenn der Systemma-

nager das Kontrollkästchen „Service“ für einen Benutzer aktiviert, kann dieser das Ereignisprotokoll mittels Chipkarte aus dem System exportieren und es mit der Software anzeigen und drucken.

**Sondertage****Vorsicht**

Gefahr von nicht erwünschten Sondertagen.  
Schlossöffnung unbeabsichtigt nicht möglich.  
Achten Sie darauf, Feiertage wie Ostern, die jedes Jahr auf ein anderes Datum fallen, nicht als „jährlich wiederkehrend“ zu markieren.

Sondertage sind Tage, an denen das System ganztägig nicht geöffnet werden kann (in allen Versionen). Jeder Öffnungsversuch, der an einem Sondertag erfolgt, wird abgebrochen. Ab TwinLock Business Firmwareversion LP08 können Sondertage auch zu Tagen definiert werden, an denen trotz anderen Zeitprogrammen ausnahmsweise ganztägig geöffnet werden darf.

Bis zu 30 Sondertage im Jahr können Sie über optionale Software definieren. Sondertage können als „alljährlich wiederkehrend“ definiert werden. Funktion „Sondertage“ setzt andere Zeitprogramme außer Kraft.

Stellen Sie vor der Aktivierung des Zeitprogramms „Sondertage“ sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind.

Einstellung ab Werk: keine Sondertage

Sperrzeit nach Terminalwechsel bei Schloss in geschlossenem Zustand  
Zeitraum von 90 Minuten, in dem ein Schloss gesperrt ist, nachdem ein Terminalwechsel durchgeführt wurde, bei dem mindestens ein Schloss geschlossen war.

Sperrzeit nach Eingabe von falschem Code

Zeitraum von einer bis zu einigen Minuten, während dem ein Schloss trotz Code-Eingabe nicht öffnet, weil ein Benutzer zuvor (wiederholt) Code falsch eingegeben hat. Je öfter falscher Code eingegeben worden ist, desto länger wird die Dauer der

Sperrzeit. Siehe auch Sperrzeit / Öffnungszeit (Zeitprogramm).

**Sperrzeit / Öffnungszeit (Zeitprogramm)**

Eine Sperrzeit ist ein Zeitraum von einem Tag bis zu zwei Monaten, während dem das System ganztägig nicht geöffnet werden kann. Für das System können Sie über PC-Software (optionales Zubehör) bis zu 3 Sperrzeiten definieren. Mit programmierter Sperrzeit wird jeder Öffnungsvorgang abgebrochen, der im definierten Zeitraum erfolgt. Sperrzeiten können auch zu einzuhaltenden Öffnungszeiten definiert werden, außerhalb denen nicht geöffnet werden kann. Werkseinstellung ist „Sperr- / Öffnungszeiten deaktiviert“. Stellen Sie vor der Aktivierung sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Siehe auch Sperrzeit nach Eingabe von falschem Code / ...bei Terminalwechsel. In allen 3 Fällen ist die Fehlermeldung „Sperrzeit“.

**Stiller Alarm**

Nur bei Eingabe von PIN-Code, nicht bei Codekarte. In einer Bedrohungssituation kann durch Eingabe eines speziellen „Alarmcodes“ beim Öffnen und Programmieren des Systems ein stiller Alarm ausgelöst werden. Das System verhält sich für Benutzer und Bedroher genauso wie beim normalen Öffnen, nur dass zugleich ein Systemmanagercode (=Managercode von Schloss 1)

**Vorsicht**

Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert. Ändern Sie werksseitige Codes sobald wie möglich. Verwenden Sie in Codes keine persönlichen Daten. Testen Sie neu programmierte Codes mehrmals bei geöffneten Wertbehältnissen.

Der Systemmanagercode, auch Systemcode genannt, berechtigt dazu, das System über die Bedieneinheit zu konfigurieren. Er wird in Schloss Nr.1 Ihres Systems gespeichert und ist Benutzer Nr.225 zugeordnet.

Werksseitig ist als Code „111111“ (bei Systemen der VdS Klasse 2) oder „11111111“ (bei Systemen der VdS Klasse 3) programmiert.

**Systemmanager**

Inhaber des Systemmanagercodes, mit dem das System konfiguriert wird. Der Systemmanager selbst kann Schlösser nicht öffnen und schließen.

**Teilsperrzeit (3 Zeiträume pro Tag)**

Stellen Sie vor der Aktivierung einer Teilsperrzeit sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Für Systeme mit zwei Schlössern können Sie über Software (optionales Zubehör) eine Teilsperrzeit mit drei Zeiträumen pro Tag definieren. Während der Teilsperrzeiten schließt nur Schloss 2, Schloss 1 bleibt offen. Mit aktivierter Teilsperrzeit wird jeder Schließvorgang von Schloss 1 abgebrochen, der in einem definierten Teilsperrzeitraum liegt. Werkseinstellung ist „Teilsperrzeit deaktiviert“.

Soll trotz aktivierter Teilsperrzeit Schloss 01 geschlossen werden:

Drücken Sie die ENTER Taste, während Schliessen | Schloss 1 Teilver- sperrt! angezeigt wird. Schloss 1 wird geschlossen, die Teilsper- rung einmalig außer Kraft gesetzt.

Funktion „Teilsperrzeit“ können Sie kombinieren mit Funktion „Automatisches Schließen mit Türschalter“. Die Folge ist, dass Schloss 1 innerhalb der Teilsperrzeit offen bleibt und nach ihrem Ende geschlossen wird.

**TwinComm**

Optionales Zubehör. Parametrierset, Software für Systeme TwinLock mit Bedieneinheit FlatControl. Die Benutzermatrix, in der die grundsätzlichen Berechtigungen für alle Benutzer festgelegt werden können, ist ein Teil der Software TwinComm.

**Wochenprogramm**

Über optionale Software können Sie bis zu 5 Wochenprogramme mit flexibel definierten Öffnungszeiträumen für jeden Wochentag einstellen. Über die

**Benutzer-**

matrix können Sie die Programme individuell Benutzern zuordnen. Mit programmier-

tem Wochenprogramm wird jeder Öffnungsvorgang abgebrochen, der nicht in einem definierten Öffnungszeitraum liegt. Stellen Sie vor der Aktivierung eines Wochenprogramms sicher, dass Uhrzeit und Datum korrekt eingestellt sind.

Ab Werk sind die Wochenprogramme deaktiviert.

**WTU-Funktion**

Siehe „Benutzergruppen“.

**Zeitprogramm**

Das Öffnen der Schlösser kann auf diverse Zeiträume beschränkt werden. Siehe auch die Einträge Sondertage, Sperrzeit, Teilsperrezeit und

**Wochenprogramm.**

Zeitprogramme / Sperrzeiten können von privilegierten Benutzern unterbrochen

den. Siehe auch „Zeitprogrammunterbrechung“ und „Schnellöffnung“.

**Zeitprogrammunterbrechung**

Eine innerhalb des gesicherten Bereichs eingeschlossene Person kann einen im Inneren des Wertbehältnisses angebrachten Druckschalter betätigen, wodurch ein Schloss trotz aktiver Zeitprogramme (Wochenprogramm, Sondertage, Sperrzeit oder Teilsperrezeit) von außen durch Benutzerautorisierung (üblicherweise Codeeingabe) geöffnet werden kann. Nach einer Öffnung werden die Zeitprogramme automatisch wieder aktiviert. Der Anschluss eines solchen Druckschalters ist nur an der optionalen Schalteinrichtung TwinAlarm möglich, nicht an der Erweiterungseinheit TwinXT (II) oder TwinXT small. Auch ohne TwinAlarm kann ein Benutzer, der vom Systemmanager zur Schnellöffnung autorisiert wurde (Benutzermatrix), trotz Zeitprogrammen öffnen. Siehe auch „Schnellöffnung“.

**Zwangsfolge (ZF)**

Möglichkeit, eine Reihenfolge festzulegen, die beim Öffnen und Schließen der Schlösser des Systems TwinLock eingehalten werden muss.

Wenn Sie die Option „Zwangsfolge“ mit PC-Software programmieren, müssen Benutzer zuerst Schloss 1, dann Schloss 2 und danach gegebenenfalls Schloss 3 öffnen. Nach der Öffnung von Schloss 1 ist das System teilgesichert (entspricht bei Option ZF dem Zustand „gesichert“), nach der Öffnung aller Schlösser ist das System entsperret und damit ungesichert.

Beim Schließen muss zuerst gegebenenfalls Schloss 3, dann Schloss 2 und zuletzt Schloss 1 geschlossen werden. Erst danach ist das System gesichert.

Werkseinstellung: keine Zwangsfolge.

# 10 Anhang

## 10.1 Abbildungsverzeichnis

Abb. 1:	Systemaufbau von Basissystem 1.1 .....	14
Abb. 2:	Systemaufbau von Basissystem 2.1 .....	15
Abb. 3:	Systemaufbau von Basissystem 3.2 .....	16
Abb. 4:	Systemaufbau von Komfortsystem 1 mit EMA .....	17
Abb. 5:	Systemaufbau von Komfortsystem 2 mit EMA .....	18
Abb. 6:	Bedieneinheit FlatControl .....	19
Abb. 7:	Schloss INSYS Lock 700 Vds2 / - 800 Vds3 / - 900 Vds4 .....	19
Abb. 8:	Busverteiler TwinConnect / TwinConnect small .....	20
Abb. 9:	Sperreinrichtung TwinXT / TwinXT small / TwinXT II .....	20
Abb. 10:	Schalteinrichtung TwinAlarm .....	21
Abb. 11:	Design-Beispiel RFID Karte .....	21
Abb. 12:	Symbol "TwinCard code access" .....	22
Abb. 13:	Symbol "TwinCard language" .....	22
Abb. 14:	Symbol "TwinCard configuration II" .....	22
Abb. 15:	Design-Beispiel einer Chipkarte TwinCard .....	22
Abb. 16:	Übersicht am Beispiel eines Systems mit FlatControl .....	23
Abb. 17:	Beispiel Startseite PC-Software TwinComm .....	26
Abb. 18:	Bedienelemente der Bedieneinheit FlatControl .....	34
Abb. 19:	Definition von Hotkeys (Beispiele) .....	35
Abb. 20:	RFID-Karten und Kartenleser .....	49
Abb. 21:	Karte und Kartenfach FlatControl .....	50
Abb. 22:	Adapterkabel mit Eingabeeinheit verbinden .....	92

!!! Irrtum und technische Änderung vorbehalten!!!

